Enhancing Cybersecurity in Public Transportation

Sponsored by the Florida Department of Transportation & National Center for Transit Research

Principal Investigator: Sean J. Barbeau, Ph.D.
Co-Principal Investigator: Jay Ligatti, Ph.D.
Research Team: Kevin Dennis and Maxat Alibayev
FDOT Project Manager: Gabrielle Matthews

CENTER FOR URBAN TRANSPORTATION RESEARCH

Outline

- **Project Subject Background**
- Project Overview and Outputs
- Transit Cybersecurity Working Groups
- Technical Workshops
  - Traffic Cabinet Technologies
  - Mobile Fare Payment Vulnerability
  - Cybersecurity in Public Transportation Workshop
- Discussion and Recommendations
- Further Research and Conclusions

Background (1)

- Transportation infrastructure is exposed to the public
- If compromised or used maliciously, the infrastructure may harm, or deny service to, users
- In 2013 the Florida Legislature requested the formation of the Florida Center for Cybersecurity (now CyberFlorida), which named "transportation" as a focus area

Background (2)

- TCRP Web-Only Document 67:
  "The sheer numbers of suddenly visible, interconnected, increasingly vital cyber components now deployed in transportation system and transit operations have ***created enormous, underappreciated complexity and significantly greater vulnerability across the entire system****… This situation is* ***poorly understood*** *by transportation system executives, program managers, employees, elected officials and regulators."*
- APTA's SS-CCS-RP-001-10 Recommended Practice:
  "Many transit agencies do not adequately address cybersecurity issues, despite the known risks."

Outline

- Background
- **Project Overview and Outputs**
- Transit Cybersecurity Working Groups
- Technical Workshops
  - Traffic Cabinet Technologies
  - Mobile Fare Payment Vulnerability
  - Cybersecurity in Public Transportation Workshop
- Discussion and Recommendations
- Further Research and Conclusions

Project Objectives

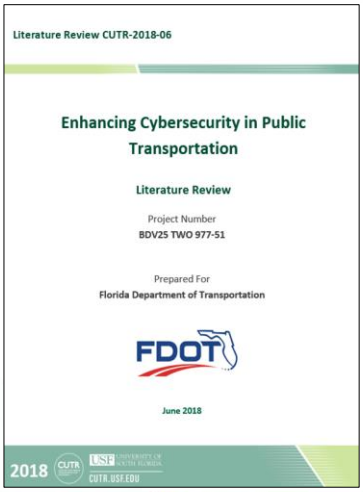
- Improve the cybersecurity of public transportation systems in Florida by:
  - Identifying and mitigating transit cybersecurity liabilities
  - Facilitating ongoing cybersecurity information exchange among Florida transit agencies, their vendors, and cybersecurity researchers
- Sponsored by the Florida Department of Transportation and National Center for Transit Research

Cybersecurity in Public Transportation

- Public transportation systems includes many technologies:
  - Onboard Wi-Fi
  - Mobile Applications (i.e. fare payment)
  - Automatic vehicle location (AVL)
  - Real-time information APIs
  - Traffic signal preemption & priority
  - Traditional IT systems
- Given the rapid adoption of technology in the area of automated and connected vehicles (AV/CV), transportation infrastructure is a particularly attractive target
  - Public transportation is early adopter of AV/CV

Literature Review

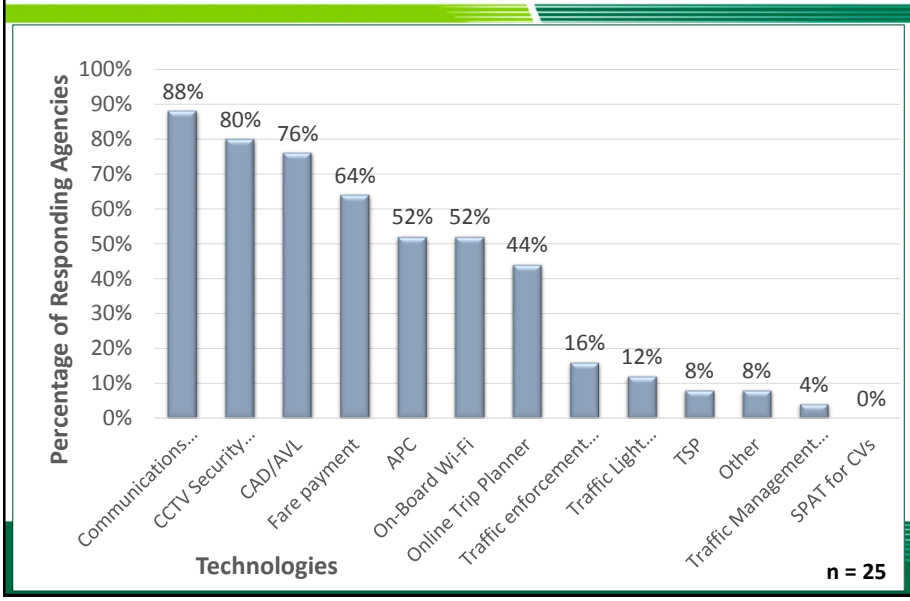
- Reviewed transit technologies (equipment and protocols) for known vulnerabilities and defenses
- Focused on technologies deployed in Florida for:
  - Fare payment
  - On-board Wi-Fi
  - Automatic Passenger Counters (APCs)
  - Automatic Vehicle Location (AVL)
  - Traffic Signal Preemption (TSP)
  - Autonomous and connected vehicles
  - General office information technology (e.g., Email)
  - Mobile apps
- Findings presented to:
  - Florida Public Transportation Association
  - Project working groups
  - Transportation Research Board 98th Annual Meeting



Survey of Florida Transit Agencies

- Surveyed 25 transit agencies across the state of Florida
- Questions focused on four key areas:
  - Current and future technology deployments
  - Current scope of AVs and CVs
  - Data management techniques
  - Experience and concerns

Survey Results – Transit Technologies Deployed in FL



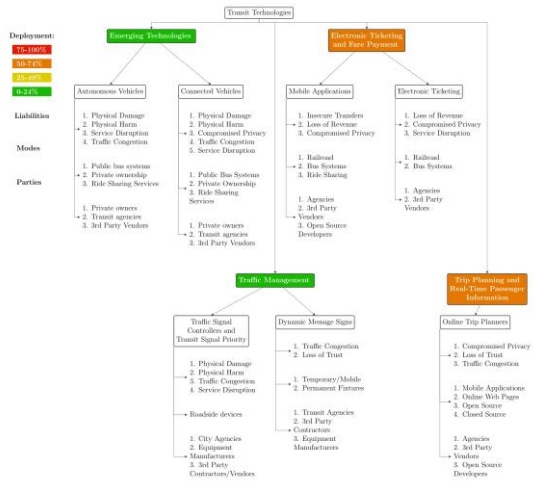
- 3 agencies responded that they have deployed AVs
  - One shut down
- 1 agency responded that they have deployed CVs
- 10 agencies planning on deploying CVs or AVs in next 6 years

Key Survey Results

- The most widely deployed technologies (communication systems, CCTV security cameras) are also considered the most operationally-critical
  - Fare payment systems = most financially-critical
- Only two agencies reported that they were impacted by cybersecurity issues
  - Website and Facebook pages compromised, phishing attempts, data theft
- Two agencies stated that they did not have any cybersecurity challenges (!)
- Commonly reported challenges for good security practices:
  1. Employee training
  2. Funding
- Approximately 40% of agencies responded that customer information wasn't encrypted, or they didn't know if it was encrypted (possibly maintained by 3rd party)
- On-board Wi-Fi may serve dual use (passenger access and transferring data off-board)

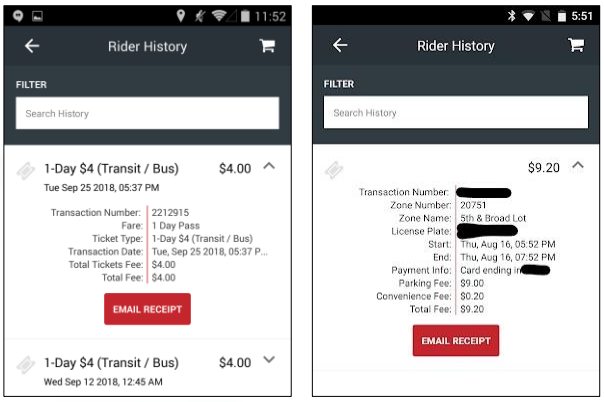
Taxonomy of Technologies

- Developed a taxonomy of transit technologies
- Taxonomy dimensions:
  - Deployment in Florida
  - Mode of transportation
  - Functionality (e.g., fare payment, APC, TSP)
  - Organization ownership
  - Security liabilities



Discovered Vulnerability in Fare Payment App

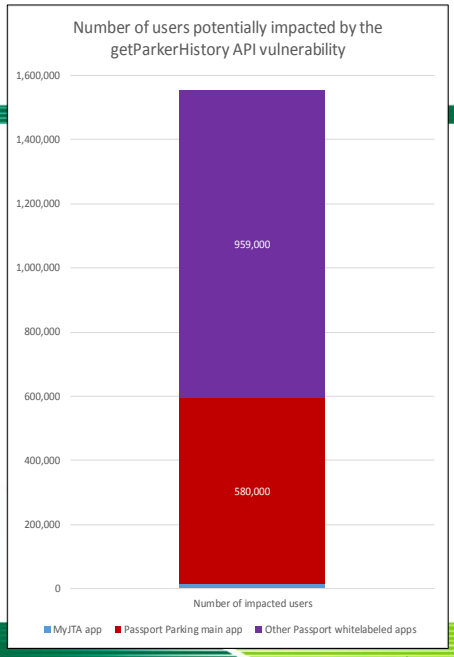
- The research team found a vulnerability in a mobile fare payment app deployed in Florida
  - An API call for rider history did not correctly validate the user & session token pair
- Personal information of users exposed:
  - Name
  - Phone number
  - Last 4 digits of credit card number
  - Vehicle info from shared database
    - License plate number
    - Parking location
- As many as 40 organizations may have been affected (transit agencies & cities)
- Patched within four weeks of being reported to vendor



Victim info viewed in app

Potential Costs if Exploited

- Transit agency app had an estimated 15,000 users
- Vulnerability affected an estimated 1,544,000 users across 40 cities when considering all apps by same vendor
- May have avoided costs on the order of millions of dollars, up to an estimated $188M (based on $121/record estimate per NCHRP)



Outline

- Project Subject Background
- Project Overview and Outputs
- **Transit Cybersecurity Working Groups**
- Technical Workshops
  - Traffic Cabinet Technologies
  - Mobile Fare Payment Vulnerability
  - Cybersecurity in Public Transportation Workshop
- Discussion and Recommendations
- Further Research and Conclusions

Transit Cybersecurity Working Group

- Planned and conducted ten web meetings over 12 months
- Stakeholders:
  - Florida transit agencies
  - Florida Center for Cybersecurity
  - Florida cybersecurity researchers
- Objectives:
  - Proactive – identify new concerns and mitigations
  - Reactive – consider existing and known vulnerabilities and best practices for preventing exploits

Transit Cybersecurity Working Group

Presentation Title	Presenter	Date
Project Overview and Survey Results	USF Research Team	7/11/2018
Continuation of Survey Results	USF Research Team	8/8/2018
Literature Review	USF Research Team	9/5/2018
Continuation of Literature Review	USF Research Team	10/3/2018
Cybersecurity for Smart Mobility Initiatives	Scott Keith (City of Tampa), Rick Tiene (Mission Secure)	11/14/2018
FDOT Regulatory Safety and Security Infrastructure	Ashley Porter (FDOT Public Transit Office)	12/12/2018
ISAC/ISAO Program	Kevin Salzer (Jacksonville Transportation Authority)	1/23/2019
SCMS for Connected Vehicles	Steven Johnson (HNTB)	2/13/2019
Mobile Fare Payment App Vulnerability	USF Research Team	3/20/2019
FDOT Triennial Compliance Review	Gennaro (Rino) Saliceto (CUTR @USF)	6/19/2019

Outline

- Project Subject Background
- Project Overview and Outputs
- Transit Cybersecurity Working Groups
- **Technical Workshops**
  - Traffic Cabinet Technologies
  - Mobile Fare Payment Vulnerability
  - Cybersecurity in Public Transportation Workshop
- Discussion and Recommendations
- Further Research and Conclusions

Organize and Host Technical Workshops

- Hosted three technical workshops aimed at identifying and evaluating potential vulnerabilities in transit technologies
- Brought together the Florida Center for Cybersecurity, students of cybersecurity, cybersecurity researchers, and Florida transit agencies

Event	Date
Mobile Fare Payment Workshop	11/9/2018
Traffic Cabinet Security Workshop	1/25/2019
Cybersecurity in Public Transportation Faculty Workshop	4/16/2019

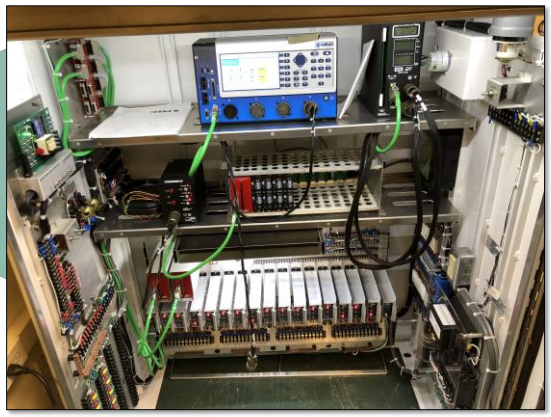
Workshop 1: Mobile Fare Payments

- Taught students Android app vulnerability analysis using hands-on transit examples
  - Included an overview of the discovered vulnerability
- Estimated attendance at 17 students, including members of the Whitehatters Computer Security Club and a representative from SOFWERX

Workshop 2: Traffic Cabinet Security

- Introduced students to traffic cabinet technologies and security
  - Included a presentation Mission Secure on potential attack scenarios
- Estimated attendance at 33 participants
- Students were encouraged to investigate the traffic cabinet, which was opened for them to interact with
  - Some students successfully placed the cabinet in a flashing state

Workshop 2: Traffic signal control cabinet



Inside of cabinet in CUTR's lab
(Donated by City of Tampa)

Vulnerabilities:

- Easy physical access
- Default or no username/password for controller
- Easy to trigger fault state (flashing red/yellow)
- No authentication or encryption for communication with TMC

Workshop 3: Faculty Workshop

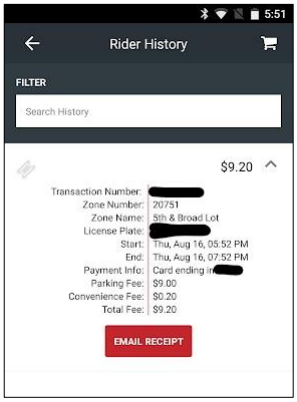
- Thirteen professors from UF, USF, FSU, and FIU were invited to present their research and discuss cybersecurity in public transportation
- Topics included
  - Privacy in intelligent transportation systems
  - Connected and autonomous vehicles
  - Denial of service attacks in transportation systems
- Transit agency employees and graduate students were invited to attend and join in on the discussion

Outline

- Project Subject Background
- Project Overview and Outputs
- Transit Cybersecurity Working Groups
- Technical Workshops
  - Traffic Cabinet Technologies
  - Mobile Fare Payment Vulnerability
  - Cybersecurity in Public Transportation Workshop
- **Discussion and Recommendations**
- Further Research and Conclusions

Vulnerability Disclosure Process

- No existing vulnerability disclosure policy existed for the agency or vendor of mobile fare payment app
  - The team reported the vulnerability to agency employee participating in cybersecurity working group
- To the team's knowledge no users or other agencies were informed by the vendor that a vulnerability leaking personal data was discovered
- A brief review of other Florida transit agencies and their vendors did not find any publicly-available responsible disclosure processes



Victim info viewed in app

Current Florida Policy

- The Florida Information Protection Act of 2014 requires government and private entities to provide notification within 30 days after a breach affecting 500 or more individuals in Florida is discovered
  - However, data from mobile fare app doesn't appear meet the statue's definition of personally identifiable information (PII)
- Other states have different laws regarding data breaches and PII definitions
- No existing federal law regarding general (non-financial or medical) data breach notifications was found by the research team
- At FDOT's request, the team has suggested additional language for FL Rule 14-90 for responsible disclosure requirements (see next slide)
- More broadly, cybersecurity could be integrated into existing safety and security requirements
  - *(e.g., policies, training, reporting, emergency management, incident investigation, documenting drills and exercises, monitoring contractors)*

Rule 14-90 language recommendation

- *(l) A public cybersecurity vulnerability disclosure policy that includes:*
  - *a single, public point of contact at the bus transit system for disclosure of vulnerability reports.*
  - *expeditious notification of any and all potentially affected or in-danger parties, including users of the system.*
  - *practical and timely steps to mitigate and recover from known vulnerabilities.*
  - *a location for prominent public display of the policy (e.g., on the agency's website).*
  - *compliance with the Florida Information Protection Act of 2014.*
- *(m) Contractual templates used by the bus transit system to engage contractors and vendors that require these entities to comply with the bus transit system public cybersecurity vulnerability disclosure policy described in Section (3)(l). Contractors and vendors shall report all known vulnerabilities to the bus transit system in a timely manner and shall describe in the contract practical and timely steps to mitigate and recover from known vulnerabilities without additional charge to the bus transit system (e.g., as part of a maintenance agreement).*

Discussion

- Publicly available vulnerability disclosure policies may allow vulnerabilities to be quickly patched and improve communication between agencies, researchers, and vendors
- Safety requirements, such as Rule 14-90, may provide starting point for introducing security requirements
  - Many processes, such as vulnerability disclosure and safety reporting, may be very similar
- Potential requirements include:
  - Standards for data encryption
  - Publicly available vulnerability disclosure policies and contacts
  - Notification of affected parties, including customers, other agencies, and vendors
  - Audits and cybersecurity employee education

Implications for agencies

- Discuss with your vendors how vulnerabilities are addressed
  - Does the vendor have a plan?
  - Will you be charged?
  - Do they inform users of breaches?
  - Do they inform agencies of breaches?
  - Do they conduct independent security audits?

Recommendations for Agencies

- Follow best-practice recommendations for mitigating vulnerabilities
  - Review existing policies and procedures
  - Use secure authentication and encryption
  - Log access to sensitive infrastructure
  - Backup critical data in case of ransomware
- Identify opportunities to improve employee training
- Create vulnerability disclosure process (internal and external)
- Track and report metrics (e.g., incidents) to FDOT
- Comply with Florida Information Protection Act of 2014 in case of data breach
- Continue to participate in information exchange with peers

Recommendations for FDOT

- Quantify and track metrics for cybersecurity incidents from agencies
- Offer resources to improve training and funding opportunities
  - These are the top two agency-reported challenges for better cybersecurity
- Consider changes to Rule 14-90 to add requirement of vulnerability disclosure process
- Consider incorporating cybersecurity into or alongside existing safety and security assessments
- Continue transit cybersecurity working group

Outline

- Project Subject Background
- Project Overview and Outputs
- Transit Cybersecurity Working Groups
- Technical Workshops
  - Traffic Cabinet Technologies
  - Mobile Fare Payment Vulnerability
  - Cybersecurity in Public Transportation Workshop
- Discussion and Recommendations
- **Further Research and Conclusions**

Further Research Needed (1)

- Develop security policies that can be widely adopted
  - Many existing safety and security processes and policies could be adapted to include cybersecurity
    - Safety reporting, auditing, etc.
  - Responsible vulnerability disclosure process
- Further investigation of vulnerabilities and mitigations
  - Evaluate security of additional transit mobile applications
  - Traffic signal controllers, traffic management centers, and traffic signal preemption/priority
  - Onboard Wi-Fi

Further Research Needed (2)

- Continued workgroups, workshops, and outreach
  - Encourage adoption of better security policies and raise agency awareness
- New surveys, based on the survey from this project, to identify and quantify the benefits of the project over time
  - Identify changes in agency behavior and policies
- Evaluate privacy concerns in transit technology
  - Mobile fare payment applications
  - Traffic signal controllers & traffic management centers
  - Onboard Wi-Fi

Conclusions (1)

- Cybersecurity is a significant concern across all industries and should be a top priority of transit agencies and FDOT
- Lack of training and funding were top cited challenges by agencies for improved cybersecurity

Conclusions (2)

- Cybersecurity policies and procedures at agencies are lacking
  - Development and implementation could be supported by FDOT (e.g. additions to Rule 19-40)
- Risks and improvements should be reported and, when possible, measured to assist with resource allocation and to track efforts to improve cybersecurity
- Many avenues for attack on existing transit systems require additional analysis
  - Existing vulnerabilities were identified for most technologies

Thank You!

Sean J. Barbeau
Center for Urban Transportation Research @ USF
barbeau@usf.edu

Jay Ligatti, Kevin Dennis
Computer Science and Engineering, USF
ligatti@cse.usf.edu, kevindennis@mail.usf.edu

CUTR

UNIVERSITY OF SOUTH FLORIDA