The Importance of Information Technology (IT) for Transportation Security

John C. Falcocchio and Rae Zimmerman

WISSP10, Abu Dhabi, October 4, 2010

This presentation is for use at WISSP10, and not for further distribution or electronic posting without the permission of authors.
Presentation Outline

I. A Brief Overview of the Transportation System
II. IT and Transportation
III. IT and Transportation Security
IV. Conclusions
V. Policy Recommendations
VI. Recommended Research Directions
I. Brief Overview of the Transportation System

Four Core Components:

- Physical Infrastructure
- Vehicles
- Operators / Operations
- Customers
Interfaces of Transportation System Components

1. Physical Infrastructure and Vehicles
2. Operators
3. Customers
II. IT and Transportation

- IT has made these interfaces more efficient by leading to the creation of an:
  - *Intelligent Infrastructure*
  - and
  - *Intelligent Vehicles*
Intelligent Infrastructure Services for Highways

- Arterial Management
- Freeway Management
- Crash Prevention and Safety
- Road Weather Management
- Roadway Operations and Management (lighting, signaling; maintenance)
- Traffic Incident Management
- Emergency Management
- Electronic Payment and Pricing
- Traveler Information
- Information Management
- Commercial Vehicles
- Intermodal Freight

How IT Interfaces with Highways:

- These services are enabled by traffic surveillance and detection techniques, such as sensors, or cameras monitoring traffic flow.
- The surveillance and detection techniques used to monitor traffic flow in support of ITS applications can also be used to monitor key transportation facilities for security purposes.
Intelligent Infrastructure Services for Transit

Include:

- Operations and Fleet Management
- Information Dissemination
- Transportation Demand Management
- Safety and Security
How IT Interfaces with Transit

• These services are enabled by automated vehicle location (AVL) systems, computer-aided dispatch (CAD) systems, computerized control of heating, ventilating and air conditioning (HVAC) systems, and remote vehicle and facility surveillance cameras

• Transit management centers can monitor in-vehicle and in-terminal surveillance systems to improve service and improve the safety and security of passengers and operators
Intelligent Vehicles Services

• **Accident Prevention/Avoidance**
  – Collision Avoidance
  – Collision Notification
  – Driver Assistance

• **Security**
  - Intrusion detection
  - Monitoring of incidents
  - Dissemination of warning messages
  - Deployment of security personnel
III. IT and Transportation Security

• In avoiding, mitigating or coping with security breaches
  – Highways
  – Transit
New York City, September 11, 2001:

- Updated all VMS signs to “Avoid Lower Manhattan” message
- Shared video feeds with NYPD
- Monitored highways and streets for emergency access
- Implemented “outbound” traffic signal patterns
Example: Advanced Traveler Information

- New York City closed to all traffic
- All crossings to New York closed
New York City, September 11, 2001: Communication averted adverse consequences such as deaths in trains in the area at the time of the attack by allowing train operators time to roll back trains or not have them start on what would have been a perilous journey (U.S. DOT, Volpe Center):

- Within a minute of the first plane hitting the north tower a train operator alerted the control center of MTA of an explosion and emergency procedures begin
- Within six minutes PATH begins emergency procedures
Transit

• London Train Bombings, 2005: CCTV enabled the authorities to initially track the perpetrators and finally apprehend them, though it was not able to avoid the attack
III. IT and Transportation Security, cont’d.

- Vulnerabilities of the *interfaces*
Interdependency of Interconnected Systems

- Information Technology
- Transportation
- Other Interconnected Systems
1. IT and Transportation

- Failures of IT from accidents produce consequences that are similar to those that might be expected from deliberate attacks.
IT/Transit Failures

- On August 20, 2003, the entire CSX transportation system shut down in 23 states due to the shut down of a computer system that monitors train movement and CSX signals; system restoration began with manual overrides (Daniels, August 20, 2003).

- On May 25, 2006, 112 Amtrak trains and 45 NJ Transit trains were disrupted when a 4 year old computer part failed to relay an order to restore power at one of the six substations providing power to the Amtrak system after electricity had been reduced for maintenance. Amtrak acted to manage such situations, for example, by having substations manned in peak hours, not reducing power capacity for maintenance, and having spare locomotives to move stalled trains (Associated Press, February 23, 2007).
2. IT and other Interconnected Systems: Energy for Transportation

- Oil and Gas Pipelines and IT
- Electricity and IT
Electric Power, IT, and Transportation

- Transportation is heavily dependent on electric power which in turn is dependent on IT.
- Electric power has also experienced outages from IT failures both from accidents and deliberate attacks.
Electric Power and IT Failures

- August 2003 Blackout. First Energy control room operators were unaware visually and audibly that an alarm had gone off, since their computer system was impaired. This delayed the detection of something going wrong with the electrical system. Subsequently, computer control servers became disabled. (U.S.-Canada Power System Outage Task Force April 2004).
Electric Power and IT Failures

• “In January 2003, the Slammer worm infected the safety monitoring system at the Davis-Besse nuclear power plant in Oak Harbor, Ohio, and replicated so fast that it disabled the system for nearly five hours. The worm knocked out the plant's central command system for six hours. A report from the North American Electric Reliability Council found that power wasn't disrupted, but the failure stopped commands to other power utilities.” (Arnone May 8, 2006)

• A false oil flow alarm shut an electricity transmission line down, causing a widespread blackout in Southern California affecting 500,000 people (Veiga September 1, 2005).
3. Methods to Quantify Dependencies and Interdependencies: Ratio Approaches

- A ratio was constructed of the time it took for an infrastructure dependent on electric power to recover and the time it took electric power to recover: \( T(i) / T(e) \)
- This was applied to various outages where infrastructure was affected and the recovery times for both electric power and the dependent infrastructure were known
- Such an approach is valuable given that the duration of outages varies considerably and even a given outage varies in time from place to place.

Results for the August 2003 Blackout: Electricity Outage Durations $T(e)$ and Affected Infrastructure Outage Duration $T(i)$

Outage Durations for the August 2003 Blackout
(Total Duration = 42-72 hours)

\[
\frac{T(i)}{T(e)}
\]

Transit-electrified Rail (NYC) 1.3
Traffic Signals (NYC) 2.6

IV. Conclusions

• Transportation security is compromised when a hacked computer will cause a crash, or when an IT system component fails because of poor maintenance or human error

• Maintenance of IT components at the interfaces of IT, Transportation, and other infrastructure systems (e.g., electric power) is a critical aspect of transportation security
V. Policy Recommendations

- Policies regarding the use of IT in critical infrastructures must take into account the benefits of IT when everything functions as expected, as well as the risks of incorporating IT when one or more of its components fail.
V. Policy Recommendations, cont’d.

- Such policies should be pervasive in marketing guidelines and regulations, since the risks can be very great
VI. Recommended Research Directions

• Review and assess international practices in maintenance and operations at the interfaces of IT, Transportation, and other Infrastructure systems for high risk locations (e.g., tunnels, bridges, stations where many lines converge)
VI. Research Directions, cont’d.

• Review and assess the skills of personnel assigned to maintain and operate critical system components

• Review and assess the reliability of funding mechanisms needed for preventive maintenance and for the safe operations of IT components
VI. Research Directions, cont’d.

- Identify best practices and recommend new policies that improve/assure IT reliability in transportation security
- Review and assess how maintenance practices are managed (who is in charge?) at the interfaces of IT and other interdependent systems and which agency has lead responsibility
VI. Research Directions, cont’d.

• Explore the feasibility of establishing an independent agency with the responsibility and authority to address the critical interconnections at the security interfaces of the transportation system, IT, and other interconnected systems
Thank You
References


• FHWA, Publication Number FHWA – HRT-10-004, Public roads, July- August 2010.


Acknowledgements

Anecdotes on IT/Transportation failures and successes and interdependencies were drawn from R. Zimmerman’s contribution to the following conference presentations and subsequent presentations:


Portions of this work were supported by an NYU-Poly seed grant, Center for Interdisciplinary Studies in Security and Privacy (CRISSP).