Introduction to Cyber Security Issues for Transportation

T3 Webinar – December 7, 2011

Michael G. Dinning
Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!
We’re Increasingly Dependent on the Digital Infrastructure

In NextGen Air Traffic Control Systems….
...Positive Train Control
Intelligent Transportation Systems
...Intermodal Ports

Terminal Operations & Management

Automated Gates

Physical Security

Crane Monitoring and Control

Wireless Devices & Tracking

John A. Volpe National Transportation Systems Center
E-enabled Vehicles Are Now the Norm
Transit Vehicles are E-enabled

RF  Cellular  Wi-Fi  WiMAX  DSRC

Control Domain
Vehicle Controls
Vehicle Diagnostics
Traffic Signal Priority
Video Surveillance
Duress Alarms
Vehicle Immobilizers

Operations Domain
Automated Dispatching
Vehicle Location
Route/Schedule Status
Passenger Counters
Stop Annunciation
Electronic Payments

Infotainment Domain
Customer use of Wi-Fi and WiMAX  Real-time Travel Info & Trip Planning
Automobiles and Trucks Are E-enabled

Source: aa1car.com
We’re Demanding Connectivity and Increasing the Potential Attack Surface

<table>
<thead>
<tr>
<th>Satellite</th>
<th>Cellular</th>
<th>WiFi</th>
<th>Radio</th>
<th>DSRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue Tooth &amp; RF</td>
<td>CD &amp; MP3</td>
<td>Mechanics’ Diagnostic Tools</td>
<td>Wireless Sensors</td>
<td></td>
</tr>
</tbody>
</table>
Cyber Security Threats are Increasing

A perfect storm of cyber attacks

Stuxnet & Duku

Cyber Attacks

Cyber War
Frequent Hacks Into Highway Dynamic Message Signs
Insider Threat Impacted Traffic Management Center & Signaling
Researchers Revealed Potential Vulnerabilities in Automobiles
Recent Hybrid Attacks on Transit

“No Justice No BART” – Physical Attacks

“Anonymous” – Cyber Attacks
Even “Isolated” Legacy Systems Are Vulnerable
14 Year Old Boy Derails Polish Trams, January 2008

- 4 light rail trains derailed, 12 people hurt
- Used modified television remote controller
- Locks disabling switch when vehicle present not installed
Need a Complete Understanding of the Systems, Interdependencies & Importance

Cyber-physical Control Systems
Traffic Control & Operations Management Systems

Safety Management Systems
Traveler & Operator Services: 511, E-commerce, E-payment

John A. Volpe National Transportation Systems Center
Must Understand Dependencies on Critical Information

Example: Fatal SpanAir Crash

• Cause: pilot error
  – Failed to deploy flaps
  – Warning disabled

• Related factor: Virus in management system
  – Virus had slowed maintenance management system
  – Data not entered
  – Would have grounded plane
Understanding and Risk Mitigation Requires Collaboration

- Designers & manufacturers
- Equipment suppliers
- System integrators
- Expert consultants
- University & government researchers
- Testing organizations
- Users (airlines)
- Infrastructure operators
- Standards organizations
- Certifiers and regulators

Example: Airborne Network Security
Best Practice: Collaboration on Airborne Network Security

Airborne Network

Equipment / Engineering

Funding / Strategic Direction

Security Simulator

Subject Matter Experts

Research / Facilities

Manufacturing
Airbus, Boeing, Bombardier, Astronautics, ARINC, CMC Electronics, Curtiss-Wright, General Electric, Panasonic, Rockwell-Collins, Thales

Airline Operations
American Airlines, British Airways, Delta Airlines, Lufthansa, United Airlines

Government

Academia
Wichita State University, Louisiana Tech University
We Must Build Security Into the Process to Ensure the Resilience of the Overall System

Risk assessments
Standards
Design practices
Certification
Maintenance & Ops

Goals: systems safety, security, reliability and resilience
Create a Cyber Security Eco System: Incorporate Security Into the Design Process, SMS’s & the Safety Culture

System security/safety process, management systems and culture

The Four SMS Components

- **Safety Policy**: Establishes senior management’s commitment to continually improving safety, defines the methods, processes, and organizational structure needed to meet safety goals.

- **Safety Assurance**: Evaluates the continued effectiveness of implemented risk control strategies, supports the identification of new hazards.

- **Safety Risk Management**: Determines the need for, and adequacy of, new or revised risk controls based on the assessment of acceptable risk.

- **Safety Promotion**: Includes training, communication, and other actions to create a positive safety culture within all levels of the workforce.

Cyber risk management throughout the systems development life cycle

Systems engineering process

Certification process

John A. Volpe National Transportation Systems Center
Strategy Must Address Life Cycle

Create a cyber security eco-system (like Fire Safety)

- Identify systems, connections & interdependencies
- Assess vulnerabilities and risks
- Identify and use best practices and standards
- Include cyber security in design specs and acquisitions
- Collaborate with IT, physical security & other groups
- Develop polices and procedures for cyber security
- Motivate employees with training, exercises & “hot triggers”
- Make sure that systems and operations are resilient (i.e. layers, detection, incident response, COOP)
- Develop organization-wide strategic plan linked to funding
Cyber Security Resources and Tools

- TSA Transportation Systems Sector Cyber Working Group
  - Newsletter, monthly meetings, summit, training, case studies
- DHS Control System Security Program - Transportation
  - Assessments (i.e. CSET), information sharing, standards, training
- Industry associations
  - APTA Control & Communications Security Working Group
  - AAR Rail Information Security Committee
  - SAE Automotive Systems Security Committee
  - RTCA SC216 Aeronautical System Security Committee
  - AAPA Security Committee
- TRB Transportation Cyber Security Sub Committee
- Information Sharing and Analysis Centers & Computer Emergency Response Teams
- DOT Volpe Center Transportation Cyber Security Team/Lab
Cyber Security is One of the Most Serious Potential Risks in Transportation

- Increasing dependence on information systems and networks
- Risks are significant and growing
- Need a comprehensive approach
- Need a culture/ecosystem of cyber security (like fire safety)
- Cyber security is necessary for transportation mobility and safety!