SPEAKER

Robert Gallamore

Northwestern University Transportation Center

“Making Rail and Container Freight More Secure: A Survey of Work in Progress”
CYBERSECURITY
OF FREIGHT INFORMATION
SYSTEMS – A SCOPING STUDY
TRB SPECIAL REPORT 274

Robert R. Gallemore, Chair
The Transportation Center at Northwestern University

Presented at: Optimizing Resource Allocation for Transportation Infrastructure Protection
University of Wisconsin – Madison
May 20, 2004

Committee Membership

- Robert R. Gallemore, Chair, Northwestern University
- A. Ray Chamberlain, Vice Chair, Parsons Brinckerhoff, Inc.
- Frank J. Anissett, Raytheon Company
- Samuel H. Banko, Sandia and Tavis
- Richard A. Holmes, Jr., Union Pacific Railroad
- Barry Horowitz, University of Virginia
- John L. King, University of Michigan
- Lars Kjaer, World Shipping Council
- Art Krouth, TransSecure LLC
- Steven J. Lambright, Savi Technology
- Daniel Murray, American Transportation Research Institute
- Frank Pittelli, Navis Technologies, LLC
- Alan F. Spear, MTC Investigator (USA), Inc.
- Karen Ryan Tobia, Port Authority of New York and New Jersey

Charge to the Committee

- Baseline Description of U.S. Freight Transport Communications and Information Systems (C&IS)
- Summary of C&IS Technology Applications and Improvement Efforts
- Summary of Potential Vulnerabilities Created by Interconnection of these Systems

Generic Tasks in Freight Transport

- Matching a Load with a Carrier
- Order Acceptance
- Work Order Delivery and Reporting
- Routing / Dispatching
- Pick-up and Delivery Confirmation
- En Route Tracking
- Transmitting Shipping Documentation
- Cargo Manifesting
- Mode Change Logging (In- and Out-Gate Checking Operations)
- Time-Keeping
- Re-Fueling
- Emergency Alerts and Reports
Freight Industry Characteristics

- Scale and Complexity of the Transport Networks
  - Diversity of Modes and Providers
  - Range of Operations
  - Multiple Points of Interconnection
  - Both Fixed Facilities and Vehicles
- Information Systems Complexity
  - Increased Dependency on Vulnerable Systems
  - Difficulty of Authenticating Users
- Public-Private Interactions
  - Multiple Security Agencies Requiring Coordination

Vulnerabilities to Cyber-Terrorism

- Network Interconnections
- Internet Communications
- Decentralized Systems
- Other Developments
  - Radio Frequency Identification Tags
  - Wireless Communications
  - Cryptography
  - Smart Cards / Tokens
  - Biometric Devices

IT Trends and Emerging Technologies

- Electronic Supply Chain Manifesting
- Real-Time Monitoring
- Decentralized System Architecture
- Embedded Processors
- Electronic Data Interchange
- Increased Reliance on the Internet
- Global Interconnection of Systems
  - Firewalls – Access Controls
  - Problems of User Authentication
Examples of Sophisticated IT Applications

- Business Data Systems
- Optimization of Routing and Redirection (Loads and Empties)
- Central Dispatching
- Crew Management
- Tracking and Tracing
- Information Flow Among Supply-Chain Collaborators (Carrier-Customer Communications)
- Information Flow to Governments
- Vehicle (and ROW) Maintenance Planning

Embedded Processors and Enabling Technologies

- Direct Transfer between Real and Cyber Worlds -- Untouched by Human Hands
- RFID Tags, Active and Passive
- E-Sensors
- Smart Seals
Committee Recommendations for DHS / TSA Transportation Cyber-Security Analysis

- **Task 1**: Determine Vulnerabilities in Freight IT Systems
  - Existing & Evolving Systems
  - Prioritization by Risk (Probability * Consequences)
  - Plus Cost & Operational Impact of Implementation
- **Task 2**: Review Current Practices for IT Security
- **Task 3**: Determine Potential for IT Security Enhancements in Transport and Logistics Sector
- **Task 4**: Analyze Policies to Reduce Cyber-Vulnerabilities
- **Task 5**: Assess Economic Impact of Cost Penalties Imposed on Freight Transport

---

Some Task 5 Issues

- What Is the Effect of Security Investments on Economic Outputs?
- Can Thin Margins in Transport Support Additional Security Mandates if Privately Borne?
- When Does Security Cost Become a Concern?
- What Form of Public Participation in Security Costs Would Be Most Effective (e.g., Tax Credits)?

---

Appendices to Report 274

A. Information Management in the International Liner Shipping Industry
B. Various Security Initiatives with Relevance to Cybersecurity in Transport
C. The *Operation Safe Commerce* Initiative
D. U.S. Bureau of Customs and Border Protection Use of IT
  - Baseline Description of Existing Systems
  - The Automated Commercial Environment (ACE)
  - International Trade Data System

---

**Thank You**

Robert E. Gallamore  
r-gallamore@northwestern.edu  
(847) 491-7286