

**Call for Papers and Presentations
Proposed Paper Session for the
2010 Transportation Research Board Annual Meeting**

Protecting our Cyber Infrastructure

Sponsored by: TRB Critical Transportation Infrastructure Committee, ABE40, Committee on Information Systems and Technology, ABJ50, National Transportation Data Programs and Requirements, ABJ10, Committee on Subcommittee on Systems Analysis, Integration and Operations Planning and Management, ABE40(2), and Subcommittee on Training, Education & Technology Transfer, ABE40(5)

The TRB Committee on Critical Transportation Infrastructure Protection [ABE40], the TRB Committee on National Transportation Data Programs and Requirements [ABJ10], the TRB Committee on Information Systems and Technology [ABJ50], the TRB Subcommittee on Systems Analysis, Integration and Operations Planning and Management [ABE40(2)], and Subcommittee on Training, Education & Technology Transfer [ABE40(5)] invite you to submit papers for the upcoming TRB Annual Meeting in 2010.

Protecting our Cyber Infrastructure

Critical transportation infrastructure is vulnerable not only to physical attacks but cyber attacks against our computer networks and IT systems as well.

In 2007, there were 37,000 attempted breaches of government and private computer systems. This is an increase of 65% from the 24,000 attempted breaches in 2006.¹ According to the FBI's latest Computer Crime Survey, 9 out of 10 organizations reported computer security incidents. Total losses amounted to \$32 million.² As recently as February, 2009, FAA's computer system was compromised when hackers stole names and Social Security numbers of FAA workers and retirees. Also, economic pressures on government agencies to decrease costs and staff may present increased opportunities for cyber crime.³ In response to this cyber threat and widespread concern about the safety of personal data, the U.S. government established the Comprehensive National Cybersecurity Initiative (CNCI).

Examples of cyber attacks against U.S. transportation systems are:

- (1) The Worcester (Massachusetts) Air Traffic Communications. In 1997, a hacker broke into a Bell Atlantic computer system, causing a crash that disabled the phone system at the airport's air traffic control tower, security

¹ Department of Homeland Security, reported in *Technology News*, September 2008

² Stephen Taub, CFO.com, January 2006

³ A McAfee report on the costs of economic espionage states that organizations are concerned about the threat of laid-off employees.

**Call for Papers and Presentations
Proposed Paper Session for the
2010 Transportation Research Board Annual Meeting**

Protecting our Cyber Infrastructure

- department, and fire department for six hours and disabled the runway light switching system.
- (2) CSX Train Signaling System. In 2003, the Sobig virus infected the CSX train control computer, shutting down the train/track signaling systems in the entire east coast of the U.S. Train services were delayed for 4 to 6 hours. The same virus also shut down the CSX Florida headquarter's signaling, dispatching and other computer systems vital to its operations.

Hacking incidents have also occurred in Toronto's subway system (where the traveler information was reprogrammed), Moscow's subway system (where hacker transferred revenue from the ticketing system). There have been reports of revenue theft from domestic transit agencies due to hackers.

The protection of infrastructure is especially important for transit agencies entrusted by the public to provide safe transportation services. Many transit agencies have been deploying or planning to deploy Transit ITS technologies such as Automatic Train Control (ATC) systems for rail transit. Furthermore, working signal systems are essential for the safe functioning of heavy rail, light rail, and commuter rail systems. They are also important for bus transit including Bus Rapid Transit systems, and for electronic fare payment mechanisms as well.

The growing connectivity and interdependency of transportation systems renders consequences of the attack hard to predict and model. While a physical attack is likely to be carried out only by terrorists or hostile foreign nation-states, cyber attacks may be carried out by a wide array of adversaries, from teenage hackers and protest groups to organized crime syndicates and terrorists. Research into consequences of cyber attacks and potential attacks on the nation's transportation systems is needed.

The types of cyber attacks that should be considered by authors include: database breaches, cyber theft including theft of fares, phishing, access to intranets, access to website administration functions, attacks on control / command centers, signal systems, electronic signage, and fare payment systems

Questions about this call for papers should be directed to Yuko Nakanishi (ynakan@aol.com), Tim Schmidt, (tim.schmidt@dot.gov), Pamela Murray-Tuite (murraytu@vt.edu), or Jeff Western (Jeffrey.western@tds.net).