Emerging Issues in Transportation Information Infrastructure Security

May 21, 1996

Summary of Proceedings

July 1996

Transportation Strategic Planning
and Analysis Office
John A. Volpe National
Transportation Systems Center

Sponsored by:
Research and Special Programs Administration
U.S. Department of Transportation

Emerging Issues in Transportation Information Infrastructure Security

I. Foreword

On October 26-27, 1995, over two hundred transportation leaders and decision-makers from around the nation convened in Cambridge, Massachusetts to participate in a two day symposium on "Challenges and Opportunities for Global Transportation in the 21st Century." The symposium was convened at the John A. Volpe National Transportation Systems Center, or Volpe Center, which is part of the Research and Special Programs Administration of the U.S. Department of Transportation. The purpose of this event was to support effective public and private sector policy decisions by focusing on the core issues that underlie several of the most challenging transportation topics now on the national agenda.

As a follow-up to this event, the Volpe Center is conducting a series of six seminars during the middle of 1996 to explore in greater detail six critical issues in transportation for the next century that were identified at the symposium. These six issues, and the planned dates for the seminars, are:

- "Emerging Issues in Transportation Information Infrastructure Security" (May 21),
- "Current and Future Applications of Tagging and Tracking Technology" (June 18),
- "Mesoscale Weather Forecasting: Technological and Institutional Challenges" (July 16),
- "Spectrum Availability and Digital Communication Links" (August 20),
- "Travel and Tourism as the World's Largest Industry: Transportation Opportunities and Challenges" (September 18), and
- "Transportation Health Effects: A Current Assessment" (October 16).

Each seminar assembles approximately 40 to 50 public and private sector experts and transportation officials to provide in-depth focus on these important issues and identify potential areas where policy changes may be required, as well as topics which could benefit from additional research and analysis. This report provides a summary of the presentations and discussions that occurred during the first of these seminars, "Emerging Issues in Transportation Information Infrastructure Security," which was held at the Volpe Center on May 21, 1996.

II. Seminar Panelists

Dr. D.K. Sharma
Administrator, Research and Special Programs Administration
U.S. Department of Transportation

Dr. Richard R. John
Director, Volpe National Transportation Systems Center
Research and Special Programs Administration
U.S. Department of Transportation

Bill Marlow
Senior Vice President
SAIC Corporation

Tom Fuhrman
National Security and International Affairs Division
Office of Science and Technology Policy
The White House

Glenda Turner
Associate Director for Infrastructure Analysis
U.S. Department of Defense

Randy Schulz
Director of National Security and Emergency Preparedness
Bell Communications Research, Inc.

John Kimmins
Project Director
Bell Communications Research, Inc.

Steve Cohn
Vice President for Network Security
BBN Corporation

Roger Molander
Senior Research Staff Member
RAND Corporation

III. Overview of the Issue

Technological advances and the drive towards maximum profitability and efficiency are leading both public and private sector transportation organizations increasingly to embed sophisticated computers and communications systems and software into their transportation operations and systems. A major consequence of this trend is that transportation is becoming more dependent on elements of the **National Information Infrastructure (NII)**. In many cases, in fact, constraints on additional physical infrastructure construction mean that gaining additional transportation capacity will depend primarily on applying these NII advances. These applications in turn are giving rise to the growth of a **Transportation Information Infrastructure (TII)**, which represents the merger of the NII and the nation's transportation system. Programs such as **Intelligent Transportation Systems (ITS)** readily reflect the importance of this trend.

However, while these information and communications technologies can significantly enhance the performance of transportation functions, they can also make them more vulnerable to loss through the deliberate compromise or sabotage of these key automated elements, or even the inadvertent failure of one or more of them. In the most extreme cases, this vulnerability creates a major potential safety threat to both cargo and lives. However, even the compromise or sabotage of non-critical applications such as financial transactions can cause significant inconvenience and economic losses. All aspects of an information system are potentially vulnerable, including the communications links, the equipment, and associated software.

The importance of an efficient and effective modern transportation system to both national security and the quality of life is indisputable. Given this fact, it is important to determine the appropriate and beneficial steps the Federal government, and the U.S. Department of Transportation (DoT) in particular, can take to identify and reduce the vulnerability of transportation systems to loss or compromise due to **information system security (ISS)** threats. Two major issue areas are included in this topic. They are: first, the information systems security threats to transportation and the vulnerabilities of transportation systems and operations to these threats; and second, effective solutions and countermeasures that can mitigate these threats and vulnerabilities.

formal exposure for the layman to information security as an academic subject in the current educational system. More significantly, many system administrators themselves - who are the first line of defense against such threats - are simply not knowledgeable enough themselves about information security. They need to be trained and empowered. Personnel and system administrators can change frequently, new procedures and safeguards are constantly being developed and introduced, and inappropriate security habits can be difficult to control. Thus, employee training and awareness programs must be done continually and not as a one-time effort.

In a number of organizations, the trend is to make their systems more 'open' and accessible both for their own employees to work from remote sites or while traveling, and for customers themselves to use the systems. Allowing wireless access to a system, for example, immediately creates additional security concerns. This is the case in a number of transportation applications, such as those using automated reservation systems or sharing information on freight shipments by Electronic Data Interchange (EDI). Ironically, this desire for more 'open' systems may bring better worker efficiency and customer benefits, but it also inevitably increases the system's vulnerabilities. Another characteristic of transportation is the limited number of diversion channels that are available in case of disruptions, as compared to electricity or telecommunications. It is easier to re-route a telephone call than a shipment of 50-foot containers, for example, if the main route is not available. This makes transportation operations particularly vulnerable.

In addition to being deliberately targeted, systems are also vulnerable to unintentional damage caused by human and design errors or natural disasters. In fact, in many cases these can pose greater threats to a system than does deliberate targeting. Fortunately, many of the basic protection methods used against such attacks are also quite helpful in guarding against unintended damage. It is also important to remember that privacy and confidentiality issues are important within the U.S. context, especially given the personalized nature of many transportation services. Thus, security procedures should be designed to maximize the privacy and confidentiality of the information.

In addition to personal privacy issues, there is also an important national security dimension to the use of transportation information systems. In this context, the Federal government is evolving an 'Infrastructure Assurance' policy framework based on the importance of a robust national infrastructure to support military operations. Because so much of the Federal national security community's needs are met by private sector industries such as transportation, telecommunications and energy, this framework requires the effective collaboration of both of these groups. This collaboration would also provide important benefits to other national goals such as counter-terrorism and responding to natural disasters. Thus, it is sensible for the Federal government to assist private sector infrastructure organizations to identify information security vulnerabilities and take actions to resolve them before they have a chance to disrupt vital national security activities.

In this context, the Federal government is studying "Strategic Information Warfare" to determine more specifically what Federal policies and activities should be in this area. "Strategic Information Warfare" is a hybrid of "Information Warfare" (in information technology) and "strategic warfare" (in politics). It recognizes that key infrastructure elements, particularly transportation, have historically been major targets during warfare. This activity includes gathering data and designing models to analyze the possible costs and countermeasures associated with a deliberate systems-based attack by a foreign government on U.S. assets such as transportation, telecommunications, financial and information systems. Various 'gaming' scenarios have been developed to heighten awareness of these issues and assist in identifying areas where additional analysis, research and policy formulation is required. In addition, a Critical Infrastructure Protection Commission has recently been formed within the Department of Justice to study the vulnerability of key U.S. infrastructure elements to both physical and electronic assault.

One early conclusion from these efforts is that it would be extremely difficult, with our current capabilities, to distinguish between intentional and inadvertent failures. Thus, we could not determine accurately whether a conscious "information warfare" attack were being made against the U.S., or prove conclusively who was responsible for the attempt. A coordinated national alert system covering the major infrastructure elements - transportation, power, telecommunications, finance and energy - could provide one means of sharing and analyzing information and responding to such an event. A related conclusion is that any data base containing, or having access to, significant information on these U.S. infrastructures would itself become a possible target, and that serious consideration must be given to limiting access to such a data base. Above all, the current situation of separate or 'stovepiped' security initiatives does not work smoothly; an overall systems approach is needed to interconnect these efforts and the information they contain.

Finally, even though there is evidence of significant potential vulnerabilities in the current NII, including transportation applications, this fact should be kept in perspective. The U.S. banking and financial sector currently suffers annually from an estimated $80 billion in losses from credit card and check fraud. However, both credit cards and checks remain vital financial tools. One should not let the existence of these potential threats deter one from using the system to benefit one's operations to the extent that one can do so, as long a proper precautions are taken.

V. Topic 2: ISS Solutions

(a) Background

Given the wide range of potential threats and vulnerabilities to the communications and information systems which support transportation, it is not surprising that an equally wide range of potential solutions and countermeasures also exists. Among the specific ISS practices and procedures that can be applied to these systems are the following:

- Quality Control which factors sound security practices into the system development process at an early stage;
- Access control on code as well as data so that only authorized users can perform specific, approved operations;
- User identification and authentication through the assignment of passwords as a minimum, but including active measures such as challenge-response identity checks;
- Protection of executable codes so that programs cannot be improperly modified by unauthorized users;
- Security logging to keep records of all security-related activities for later auditing;
- Security administrators as a special category of users authorized to alter the security status of the system;
- Data encryption as a standard practice, particularly in distributed systems;
- Operational support tools that can perform inspections of security logs and security status, warn against unexpected system behavior, and control the system inventory;
- Independent audits at unannounced intervals by an outside authority; and
- Hazard analyses performed for every safety-critical system, such as situations where a life may be endangered by a failure.

However, an effective approach to providing these measures needs to cover both the technical and the non-technical aspects, including such areas as policies, procedures, training and institutional coordination. Improving the security practices for one system may be of limited use if it can be easily accessed through another, unguarded pathway. Established and well-publicized written procedures, as well as regular awareness training for all users, can also enhance overall system security.

It is also important to guard against unsubstantiated optimism over one's ISS status. One of the primary reasons for the growing concern over information security issues is the existence of a 'hacker' community which continues to 'target' vulnerable systems for unauthorized access. ISS specialists are constantly trying to stay one step ahead of the 'hacker' community, who are in turn constantly trying to foil the latest ISS practice that is developed. And it is doubtful that this spiral will ever be effectively ended. Thus, it is important for the ISS community and system users not to set 'victory' as the goal, but rather to maintain continual monitoring of their systems and to continue developing and implementing improved ISS measures.

(b) Discussion

There are a number of sectors of the economy that are becoming increasingly dependent on information networks; these include transportation as well as electric power, pipelines, water, telecommunications, and banking and finance. Transportation's two distinctions are: first, that it delivers a more personalized service tailored to the individual user's specific needs; and second, that transportation's dependence on information systems is intensifying, with many new applications just beginning to emerge. Thus, transportation users have the advantage of being in a position to build better security into their systems from the start.

In doing so, transportation can take advantage of the considerable effort already expended on information security by these other areas, particularly telecommunications and finance, and adopt the methods, equipment and procedures they have already pioneered. The telecommunications industry in particular has been targeted in a number of incidents, and has developed a strong knowledge base. They have education and training procedures, a continuing evolution of tools, and strong informal albeit private contacts within the industry. In addition, both transportation and telecommunications operate in similar environments; they are both distributed systems with little central control.

One approach to analyzing a network's possible vulnerabilities includes five steps. First, determine the operational dependencies of the network. Second, understand the network's architecture and data flows. Allowing access to one's network through another public network or the Internet, for example, means that one does not have a 'closed' system. Many individuals who think of themselves as having such 'closed' systems are, in fact, usually wrong. Third, understand the network's nodes and components. Each specific piece of hardware or software application has its own vulnerabilities which should be understood for information security procedures to be effective. Fourth, for the same reason, look at the signal protocols and transmission methods being used. Finally, thoroughly understand the existing approach to security, so that it can be assessed and improved where needed. Regular security procedures should be based on 'open' concepts that non-technical staff, including managers and supervisors, can readily comprehend, as opposed to more complicated practices that may be difficult for users to implement accurately.

SEMINAR PARTICIPANTS

Mr. John Allen
Vice President
Marketing
Battelle Memorial Laboratories
3 Cambridge Center
Suite 204
Cambridge, MA 02142
Phone: 617-577-7250
Fax: 617-577-7257

Ms. Jennifer Antonielli
Special Assistant to the Administrator
Research and Special Programs Administration
U.S. Department of Transportation
400 7th St., SW
DRP-1, Room 8410
Washington, DC 20590
Phone: 202-366-0843
Fax: 202-366-3666

Ms. Ellen Bell
Management and Program Analyst, DTS-24
Transportation Strategic Planning & Analysis Office
U.S. Department of Transportation
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: 617-494-3465
Fax: 617-494-4688

Mr. Bernard E. Blood
Chief, DTS-24
Transportation Strategic Planning & Analysis Office
U.S. Department of Transportation
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: 617-494-3454
Fax: 617-494-3688

Mr. David Cleveland
Senior Principal Engineer
ARINC
1280 Maryland Ave., SW
Box #7
Washington, DC 20024-2142
Phone: 202-651-2321
Fax: 202-484-4460

Mr. Steve Cohn
Vice President for Network Security
BBN Corporation
87 Fawcett St.
Cambridge, MA 02138
Phone: 617-873-3876
Fax: 617-873-4086

Ms. Linda Daugherty
Compliance Officer, Office of Pipeline Safety
Research and Special Programs Administration
U.S. Department of Transportation
400 7th St., SW
Washington, DC 20590
Phone: 202-366-4577
Fax: 202-366-4566

Mr. Mike Dinning
Chief, DTS-38
Safety and Security Systems Division
U.S. Department of Transportation
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: 617-494-2422
Fax: 617-494-2684

Mr. Jim Powers
Manager
Operations Center
Federal Aviation Administration
12 New England Executive Park
Burlington, MA 02803
Phone: 617-238-7001
Fax: 617-238-7007

Mr. Robert C. Ricci
Deputy Director, DTS-41
Office of Research and Analysis
U.S. Department of Transportation
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: 617-494-2343
Fax: 617-494-3064

Mr. Al Roberts
Associate Administrator for Hazardous Material Safety
Research and Special Programs Administration
U.S. Department of Transportation
400 7th St., SW
DHM-1, Room 8420
Washington, DC 20590
Phone: 202-366-0656
Fax: 202-366-5713

Mr. Don Roberts
ITS Project Team Manager
MITRETEK Systems
600 Maryland Ave., SW
Suite 755
Washington, DC 20024
Phone: 202-863-2976
Fax: 202-863-2988

Mr. Mark Safford
Management & Program Analyst, DTS-24
Transportation Strategic Planning & Analysis Office
U.S. Department of Transportation
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: 617-494-3411
Fax: 617-494-3688

Mr. Randall Schultz
Director for National Security and Emergency Preparedness
Bell Communications Research, Inc.
2101 L Street, NW
Room 700
Washington, DC 20037-1585
Phone: 202-955-4707
Fax: 202-955-4619

Dr. Dharmendra K. Sharma
Administrator
Research and Special Programs Administration
U.S. Department of Transportation
400 7th St., SW
DRP-1, Room 8410
Washington, DC 20590
Phone: 202-366-4433
Fax: 202-366-3666

Dr. Frank F. Tung
Deputy Director, DTS-2
U.S. Department of Transportation
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: 617-494-2333
Fax: 617-494-3731

Ms. Glenda Turner
Associate Director for Infrastructure Analysis
ODTUSD(P)/PS/EPP/IP
The Pentagon
Room 1D464
Washington, DC 20301-2200
Phone: 703-614-2616
Fax: 703-695-1978

Mr. Walter F. Wall, Jr.
Program Manager
Federal Aviation Administration
William J. Hughes Technical Center
AAR-510
Atlantic City International Airport, NJ 08405
Phone: 609-485-5731
Fax: 609-383-1973

Mr. Alan White
Automated Information Security and Physical Security
Federal Aviation Administration
12 New England Executive Park
Burlington, MA 01803
Phone: 617-238-7707
Fax: 617-238-7716

Mr. Howard Winkler
EG&G Dynatrend
Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142
Phone: 617-494-3446
Fax: 617-494-2957