FINAL REPORT

SURVIVABILITY OF INTELLIGENT TRANSPORTATION SYSTEMS

Brian L. Smith, Ph.D.
Faculty Research Scientist

Robert S. Sielken
Graduate Research Assistant

(The opinions, findings, and conclusions expressed in this
report are those of the authors and not necessarily
those of the sponsoring agencies.)

(Virginia Transportation Research Council
(A Cooperative Organization Sponsored Jointly by the
Virginia Department of Transportation and
the University of Virginia)

In Cooperation with the U.S. Department of Transportation
Federal Highway Administration

Charlottesville, Virginia

October 1999
VTRC 00-R9

ABSTRACT

Intelligent Transportation Systems (ITS) are being deployed around the world to improve the safety and efficiency of surface transportation through the application of advanced information technology. The introduction of ITS exposes the transportation system to new vulnerabilities, such as cyber attack. In order to ensure that ITS fulfills its potential, it is imperative that those implementing such systems design and operate them to survive cyber attacks and other information technology-related threats. Information system survivability is defined as the capability of a system to fulfill its mission in a timely manner in the presence of attacks, failures, or accidents. While total survivability may not be achievable, it can be greatly increased with conscientious efforts.

This study reviewed previous survivability research on ITS and information systems, examined the National ITS Architecture for survivability issues, and performed case studies of a number of regional ITS systems. Results from these sources were synthesized into the final recommendations contained in this report. These recommendations include:

> *Requirements: Resistance, Recognition, Recovery, and Adaptation.* VDOT should include requirements in the categories of resistance, recognition, recovery, and adaptation in all future system requests for proposals (RFPs).
>
> *Survivability Program.* Each ITS system should have a survivability program that includes both technical and nontechnical elements.
>
> *Best practices.* In addition to proper requirements and a survivability program, the best practices developed for general information technology applications should be used. Best practices include security (physical and system), design/requirements, redundancy, system configuration, and the principle of least privilege.

FINAL REPORT

SURVIVABILITY OF INTELLIGENT TRANSPORTATION SYSTEMS

Brian L. Smith, Ph.D.
Faculty Research Scientist

Robert S. Sielken
Graduate Research Assistant

INTRODUCTION

Intelligent Transportation Systems (ITS) are being deployed around the world to improve the safety and efficiency of surface transportation through the application of advanced information technology. There are many ITS benefits that have been documented over the past several years. However, the introduction of ITS exposes transportation systems to new vulnerabilities. One very real risk that ITS introduces is that of cyber attack. Attacking the transportation infrastructure can now be accomplished by attacking these ITS information systems in a manner similar to how computer hackers attempt to break into other information systems, such as banking systems. For example, attackers could conceivably gain access to the signal control system of a major metropolitan area and issue commands that set all of the signals to flash. In this scenario, attackers may not even have to leave their offices; this reduced cost barrier to carry out such attacks admits many more people to the realm of possible attackers.

Currently, the major national ITS initiative is to integrate individual ITS systems on a regional basis. Unfortunately, such integration may further increase the likelihood of cascading failures, where failures from one domain (such as an emergency services' computer-aided dispatch system) carry over into other domains (such as freeway management systems). In the United States, a recent report, the *President's Commission on Critical Infrastructure Protection* (1997), detailed the vulnerabilities of vital infrastructures, including surface transportation. *Presidential Decision Directive 63* (1998) was the President's response to the commission's report, further illustrating that this is a current issue that must be directly addressed.

Information system survivability, which can be defined as the capability of a system to fulfill its mission in a timely manner in the presence of attacks, failures, or accidents, is an area of great activity. In order to ensure that ITS fulfills its potential, it is imperative that those implementing such systems design them to be survivable. While total survivability may not be achievable in a world full of infinite possibilities for disaster, survivability can be greatly increased with conscientious efforts. Research and development in general information system survivability is still in the early stages, and very little work has been dedicated to specific ITS survivability issues. Therefore, while it is impractical to attempt to derive authoritative survivability techniques for ITS, it is important to delve into the general issues of this topic and to increase the awareness of survivability within the transportation industry.

PURPOSE AND SCOPE

The purpose of this research was increase awareness of the vulnerabilities potentially introduced by ITS and to identify general design requirements and best practices to improve the survivability of the Virginia Department of Transportation (VDOT) ITS systems.

Case studies used in the survivability analysis were confined to regional ITS projects and systems. However, identifying and reporting on specific deficiencies of the systems was not an element of the project. Such an exercise would have posed significant risks to VDOT and its systems. To meet the purpose of the study, the cases were used to identify general survivability issues and derive broad survivability recommendations that apply to ITS in Virginia and nationwide.

METHODS

The methodology used to conduct this effort is described below.

1. *Literature review of information system survivability*. This was a review of scholarly journals, technical reports, conference proceedings, and web pages. Since ITS is the application of information systems to the transportation infrastructure, it is natural to review the literature on survivability of information systems in general. The literature review included academic journal articles and technical reports in many areas of survivability, including system requirements, attack classifications, intrusion detection, mechanisms for achieving more survivable systems, and best practices. This review provides knowledge of the state of the practice and state of the art in survivability that can then be applied to ITS analysis.

2. *Review of National ITS Architecture to identify general ITS survivability issues*. The National ITS Architecture (NITSA) is a high-level framework intended to guide the implementation of ITS into regional transportation systems and to ensure compatibility with ITS in other regions of the country. The purpose of this review was to ascertain what general survivability issues have been addressed by NITSA, and which issues were not addressed sufficiently.

3. *Select Systems for Case Studies.* Four regional ITS systems were chosen for in-depth survivability analysis. The systems were chosen to provide a group as diverse in size and functionality as possible. The systems included both completely owned and maintained networks and leased lines maintained by both the customer and the provider. The systems also ranged from those only providing one or two services to systems providing more than ten services. Systems were also selected that include both information collection as well as dissemination components. Finally, case study systems were selected to include either systems that consisted exclusively of custom software or systems that were comprised only of commercial software—or systems that were made up of some combination of these two types of systems.

4. *Conduct case studies.* Site visits to the systems selected in Task 3 were conducted in order to achieve a thorough understanding of the systems. During these site visits, interviews were held to better understand how the systems were designed, implemented, maintained, and actually used. The system operators were also asked what attacks, successful or unsuccessful, have been attempted against their systems, and how these attacks were handled. The systems operators were also questioned about what aspects of their system worked well, and which aspects needed to be improved or replaced. To avoid posing an additional risk to these systems, we have masked the actual systems for this report. Therefore, although many recommendations may come from specific case studies, these studies will not be identified. The recommendations should be applicable to many similar systems as well as the actual case study system.

5. *Synthesis.* The information obtained from the previous tasks was synthesized to develop survivability recommendations for system design and system operations.

RESULTS AND DISCUSSION

Literature Review

What is Information System Survivability?

Survivability is the capability of an information system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. *Mission* is the set of very high-level requirements or goals. *Timely* is normally included in or implied by the high-level requirements. *Attacks* are potentially damaging events orchestrated by an intelligent adversary. *Failures* are potentially damaging events caused by deficiencies in the system or an external element that the system depends upon. *Accidents* are randomly occurring, potentially damaging events such as natural disasters (Ellison et al., 1997). Survivability includes the related fields of security (which traditionally includes availability, integrity, and confidentiality of information systems services), fault tolerance, safety, and reliability.

Many people mistakenly equate survivability to security, but security is actually a subset of survivability. Security exists for systems that have a central administrator and knowledge of all elements in a network. Survivability must deal with unbounded network situations that have no central administration and a lack of global visibility, such as a set of integrated ITS systems in a region. This set of ITS systems may include a freeway management system, multiple local signal control systems, police computer-aided dispatch, and an electronic toll collection system. Security demands that each node in a network such as this remain uncompromised and that each aspect of the service must also survive. Survivability can allow any individual node to become compromised while the essential services are able to continue to survive. Security is concerned only with the property of hardness that involves building a virtual wall around the network, yet trusting all those persons within the wall to behave appropriately; thus, if intruders were to get into a system, they would have basically free reign within the system. Survivability extends the hardness property to include robustness that involves additional checks within the hardness wall to keep both internal users and external intruders from abusing the system.

Survivability Objectives of Information Systems

Information systems contain three elements that must be protected: hardware, software, and communication (networks). The objectives in protecting a system include the following (Biesecker and Staples, 1997):

Confidentiality–Ensuring that the data and system are not disclosed to unauthorized individuals, processes, or systems.

Integrity–Ensuring that the data is preserved in regard to its meaning, completeness, consistency, intended use, and correlation to its representation.

Availability–Ensuring that the data and system are accessible and usable to authorized individuals and/or processes.

Accountability–Ensuring that transactions are recorded so that events may be recreated and traced to users or processes.

Threats to Information Systems

The following categories represent the general threats to information systems (Biesecker et al., 1997). These threats apply to all information systems, including ITS.

Denial of Service–Action or a series of actions that prevent some part of a system from performing as intended.

Disclosure–Unauthorized acquisition of sensitive information.

Manipulation–Improper modification of system information, whether it is being processed, stored, or transmitted.

Masqueraders–Attempts by an unauthorized user or process to gain access to a system by posing as an authorized entity.

Replay–Retransmission of valid messages under invalid circumstances to produce unauthorized effects.

Repudiation–Successful denial of an action.

The following table (Table 1) (Biesecker et al., 1997) illustrates how specific threats can be mapped into these six categories.

Table 1. Threat Category Associations.

Threats	**Denial of Service**	**Disclosure**	**Manipulation**	**Masquerading**	**Replay**	**Repudiation**
Natural Disaster						
Acts of Nature	X					
Accidental Threats						
Accidental Disclosure		X				
Configuration Error	X	X	X			
Electrical Disturbance	X		X		X	
Electrical Interruption	X					
Environmental Failure	X					
Fire	X					
Hardware Failure	X		X		X	
Liquid Leakage	X					
Operator/User Error	X	X	X	X		X
Resource Consumption	X					
Software Error	X	X	X	X	X	X
Telecommunications Interruption	X		X		X	
Intentional Threats						
Alteration of Data	X	X	X	X	X	X
Alteration of Software	X	X	X	X	X	X
Bomb Threat	X					
Eavesdropping		X				
Employee Sabotage	X		X			
Enemy Overrun	X	X	X			
Fraud			X	X	X	X
Intentional Disclosure		X		X		
Resource Consumption	X					
Riot/Civil Disorder	X	X	X			
Strike	X	X	X	X		
Terrorism	X	X	X			
Theft	X	X	X			
Unauthorized Use	X	X	X	X	X	X
Vandalism	X	X	X			

These threats exist at many levels, depending on the system. Threats may be specific to center, roadside, and/or vehicle components of ITS (Ruby et. al, 1997a). Attacks may focus on the hardware, operating system, network, or application levels of the system. Risks will vary, depending on the system. An electronic toll collection system may be concerned with the disclosure of sensitive information, denial of service (loss of revenue), manipulation, and repudiation. On the other hand, a freeway management system or signal control system may only be concerned with denial of service and manipulation of information.

Categories of Requirements

To make information systems more survivable, the system must be designed to prevent intruders from gaining access to the system and to identify intruders that were able to bypass the protection devices. An intrusion usually involves three phases.

Penetration–The intruder gains access to the system in some manner (cracking an operator's password, coercing a DOT employee, etc.)

Exploration–The intruder investigates the system to identify what services are being run on the system and hence where the vulnerabilities may lie, such as modems and unprotected access points.

Exploitation–The intruder uses the information from the exploration phase to inflict damage to the system.

To combat intrusions, four general categories of requirements are necessary for detection and identification (Ellison et al., 1997).

Resistance–The capability of the system to deter attacks (used to fight the first two phases of an intrusion).

Recognition–The capability of the system to recognize that an attack has taken or is taking place (used to combat all three intrusion phases).

Recovery–The capability of the system to regain service after an attack.

Adaptation–The system is altered to avoid such attacks again in the future.

To accomplish the system's mission, there are services that are vital and non-vital to this mission being fulfilled (Ellison et al., 1997).

Essential services–Those system functions that must be maintained in a potentially intruded environment. If an essential service is lost, it must be replaced with another service that supports the fulfillment of the mission.

Nonessential services–Those system functions that may be suspended during hostile times since, while they provide useful services, they are not essential to fulfilling the system's mission.

For example, a traffic signal system is frequently considered the most important service that an ITS provides. Thus, it would be classified as an essential service, since failure of the signal control system would be catastrophic. If the system also operates a web page, it may be considered a nonessential service, since its failure for a short period of time would be inconvenient but not disastrous. During an attack, all services may not be sustainable, and the system may have to choose which services must be maintained and which services could be temporarily suspended so that the essential services can continue to be provided.

Survivability Program

Information technology professionals advocate the implementation of formal survivability programs to guide large-scale information systems. Such a program directly addresses both technical and nontechnical issues. The following attributes (Biesecker, et al., 1997) demonstrate what elements are generally included in a survivability program.

Technical

Confidentiality–Restricts access to sensitive information (normally through encryption).

Authentication–Verifies one's identity.

Data integrity–Ensures that information is not modified while it is being stored or transmitted except by authorized individuals.

Non-Repudiation–Prohibits the sender or receiver from later denying the action.

Access control–Regulates who has access to what, and what they can do with it once they have access to it.

Accountability–Attributes actions to those who performed them.

Availability–Ensures that the resources are available for their intended use and are performed as expected.

Nontechnical

Administrative–Proper management of information throughout an organization.

Personnel –Limiting employees' access as appropriate, based on their responsibilities.

Physical–Protection of buildings, offices, and equipment from harm, destruction, or unauthorized physical access.

In addition to covering these issues, if an organization wishes to have any legal clout in prosecuting intruders, an acceptable use policy is necessary. Otherwise, enforcement becomes very difficult.

The following table (Table 2) shows some elements of a survivability program that counteract the threats to the system mentioned in the previous section. An ‘X’ indicates that the element of the program can be used to protect against attacks of the type indicated by the row.

Table 2. Threats Vs. Services.

Threats	**Confidentiality**	**Authentication**	**Integrity**	**Non-Repudiation**	**Access Control**	**Auditing**	**Availability**
Denial of Service					X		X
Disclosure	X				X		
Manipulation			X		X	X	
Masquerading		X					
Replay		X					
Repudiation				X			

Intrusion Detection

In addition to the categories of requirements that resulted from the three phases of an intrusion, an automated intrusion detection system (IDS) can be built to detect intrusions at any of the three phases. Intrusion *detection* involves determining that some entity, an *intruder*, has attempted to gain access, or worse yet, has actually gained unauthorized access to the system. Intruders are classified into two groups. External intruders do not have any authorized access to the system they attack. Internal intruders have some authority, but seek to gain an additional ability to take action without legitimate authorization (Anderson, 1980). Currently there are two basic approaches to intrusion detection. The first approach is to define and characterize the correct static form and/or acceptable dynamic behavior of the system, and then to detect abnormal behavior by defining statistical relations. This is called anomaly detection. It relies on being able to define the desired form or behavior of the system, and then to distinguish between that definition and undesirable form or anomalous behavior. While the boundary between acceptable and anomalous forms of stored code and data can frequently be precisely defined, the boundary between acceptable and anomalous behavior is much more difficult to define. The second approach, called misuse detection, involves characterizing known ways to penetrate a system, usually described as a pattern, and then monitoring for the pattern by defining rule-based relations to detect the pattern.

Intrusion detection has traditionally been performed at the operating system (OS) level by comparing expected and observed system resource usage. OS intrusion detection systems can only detect internal or external intruders who perform specific system actions in a specific sequence or those intruders whose behavior pattern statistically varies from a norm. An example of this would be a user who continually attempts to access the variable message creation portion of a freeway management system when he/she does not normally perform this function. Since internal intruders have some access to the system, they may act within their bounds of authorization; however, they may actually be abusing the system. Detection of these abusers is extremely difficult because their actions may be legitimate under certain conditions. Internal intruders are said to comprise at least fifty percent of intruders (ODS Networks, 1999); however, unfortunately, OS intrusion detection systems are frequently insufficient to catch such intruders since they neither significantly deviate from expected behavior nor do they perform specific intrusive actions, since they are already legitimate users of the system. Therefore, current research has attempted to detect intrusions at the level of the application. The hypothesis is that application-specific intrusion detection systems can use the semantics of the application to detect more subtle, stealth-like attacks such as those carried out by internal intruders who possess legitimate access to the system and its data, and who are acting within the bounds of normal behavior, yet who are in actuality abusing the system.

Limitations of Security Mechanisms

There have been many security mechanisms developed that are effective in providing the service for which they were designed. A *firewall* is a collection of hardware and software components placed between networks to protect one network from another. Therefore, a firewall only provides access control and should not be used for authentication.

Encryption is the process of disguising data so that it cannot be read unless the data is decrypted. Encryption can provide confidentiality, authentication, integrity, and non-repudiation (Biesecker and Staples, 1997). While encryption can theoretically provide all of these services, there are some problem with encryption if it is not implemented and utilized properly. Implementation weaknesses include buffer overflows, secrets not being erased properly, and poor error-checking and recovery. Replay attacks can be a problem, since the attacker does not have to decrypt the message as long as the attacker can figure out the purpose of the message. Plain text, the message in its unencrypted form, can be a problem when it is not properly destroyed after encryption. This plain text may be left over in a file, a temporary file, or in virtual memory (Schneier, 1998). Also, the more encrypted messages that are available to the attacker, the more likely that they could be deciphered. Hence, encryption should only be used for information that is considered sensitive, and the keys used for encryption and decryption should be changed frequently in a secure manner. Encryption can also be used in creating *digital signatures*, a security mechanism that is the electronic equivalent of a handwritten signature and can be attached to electronic transactions. Digital signatures can provide non-repudiation, authentication, and integrity.

National ITS Architecture

The National ITS Architecture (NITSA) is a high-level framework intended to guide the incorporation of ITS into regional transportation systems and to ensure compatibility with other ITS in other regions of the country. The most effective time to build survivability into a system is from the beginning. Given that the anticipated Federal policy will require NITSA compliance, NITSA should have a survivability component to provide some direction in helping the system designers and maintainers to build and maintain more survivable systems.

By analyzing NITSA, we were able to identify ITS examples of the six threats described previously.

Denial of Service could be performed on a traffic signal control system by an attacker connecting with the modem in the field controller and repeatedly initiating a system self-check which would bog the system down to the point that it could not respond to other commands.

Disclosure of privileged information in a commercial fleet management system could lead to a competitor gaining a competitive advantage over another company.

Manipulation of information in an electronic toll collection system could allow a person to obtain free service by having some other account charged for the service.

A *masquerader* could attack the system by acting as an emergency vehicle by preempting traffic lights.

Replay of valid commands at invalid times could lead an attacker to have control over restricted lanes by being able to open and close the gates at will.

Repudiation could be performed by a public transportation passenger who uses the public transportation and then claims that they were charged for services that they did not use; without proof that the passenger used the system, the public transportation system would have to absorb the loss because it could not prove that the services were delivered.

CONCLUSIONS

A security report analyzing each ITS system and subsystem of NITSA has been completed (Biesecker, et al., 1997). The report analyzed NITSA's subsystems, data flows, and communication infrastructures. The nineteen subsystems were analyzed by predicting the impact of each of the six threats: denial of service, disclosure, manipulation, masqueraders, replay, and repudiation. The analysis resulted in seven main conclusions.

1. There is neither a security architecture nor a security policy for ITS that articulates the ITS security objectives which would lead to survivability-related requirements.

2. There were many different types of attacks that would affect the system.

3. ITS includes both essential and nonessential services. This allows for a prioritization in system design to be achieved that provides graceful system degradation.

4. Personnel who operate the systems should be properly trained and managed.

5. The distributed nature of ITS and the communication between subsystems make denial of service attacks a major concern; this promotes the need for an incident management plan to recover from an attack.

6. Various types of data should be subdivided according to the protection required.

7. The hardware and software of the systems should be inter-operable using the appropriate standards and protocols.

These conclusions support many of the observations obtained from our literature review and reinforced many of the observations derived from the case studies to be discussed next.

GENERAL ITS SURVIVABILITY RECOMMENDATIONS

Several case studies were chosen to portray a group as diverse in size and functionality as possible. The systems chosen include a signal control system, traffic management centers, and an electronic toll-collection system. The traffic management centers were similar in some aspects, but included different functional capabilities. All of these systems used multiple computers to control hundreds of devices distributed throughout the transportation infrastructure. Thus, to avoid posing an additional risk to these systems, the identity of the actual systems will not be revealed. Rather than discuss general case study observations next, and risking the revelation of particular system vulnerabilities, this section describes general ITS survivability recommendations derived from the literature review, study of NITSA, and the case studies.

The survivability of ITS is a serious issue and one that will grow in importance as the regional integration of ITS systems accelerates. There is no magic bullet to provide ITS survivability. It is important that VDOT becomes familiar with the issues associated with information systems survivability, and takes a vigilant approach to this area. Key areas that require VDOT's attention are:

Requirements – Resistance, Recognition, Recovery, and Adaptation. For all new systems, VDOT should stipulate functional requirements in the categories of resistance, recognition, recovery, and adaptation.

- Resistance requirements should include requirements regarding backups and redundancy as well as software fault tolerance.

- Recognition should include an auditing procedure for investigations by personnel as well as automated auditing and/or intrusion detection.

- Recovery requirements will involve the development of the procedures to be used to recover from an incident and affect the choices of system hardware devices, since the hardware limits how quickly a system can recover.

- Adaptation requirements should indicate who is responsible for updating the system so that similar future attacks are thwarted successfully.

Survivability Program. Sound operating procedures are needed for survivability. Therefore, each ITS system should have a survivability program that includes both technical and nontechnical elements. Since this program will include a disaster recovery component, it must be system-specific. However, the components of the program could be used in a system-wide fashion to make sure that each system has a survivability program that is extensive enough to be useful. Because the programs are system-specific, the system operators and managers of each system should be responsible for the program. Although it will require periodic updating, the updates should be able to be completed in a couple of days unless the system has undergone significant transformation since the last update.

NITSA Survivability. Given the prominent role that NITSA will most likely play in future federally funded ITS projects, the absence of a survivability component is a significant problem. VDOT should request FHWA to initiate an effort to add a survivability component to NITSA before mandatory compliance regulations are adopted.

In addition to proper requirements and a survivability program, the best practices developed for general information technology applications should be used. The general ITS survivability best practice recommendations are presented in the following categories: security, design/requirements, redundancy, system configuration, and principle of least privilege.

Security

Security through obscurity, the assumption that keeping information about the system under close surveillance will not work since somebody will eventually find out enough information (maybe through a former employee or an intrusion) to cause a disturbance. It is the overall mission that must survive, not necessarily each particular portion of the system. Individual nodes, or distinct subsystems of an information system, should generally contribute to the survivability goals, and at worst, not interfere with these goals. Everybody involved with ITS should be concerned about information security. This includes the system owners, developers, managers, operators, users, and the public. The system must be protected at the software, hardware, and network levels. Physical security and proper security management are just as important as computer system security, because either one of those can undermine the best computer security system.

Design/Requirements

Because survivability is more easily achieved at the time the system is designed, the initial system requirements should reflect this goal. Specific requirements may include a quantitatively specified error rate, percentage of availability, reliability, and maximum outage duration. These requirements will influence the type of system installed and the manner in which it is installed. For example, the installation of the communications media significantly impacts both service and maintenance. Wires or fiber that are not buried at the proper depth will result in too many wire cuts affecting the availability and reliability of the system. The system should also be deployed in a manner that helps with fault isolation, since the time to isolate the fault is frequently the largest portion of the time of degraded service. System manuals including a diagram of the system are important not only for training new personnel, but also for maintaining the system and providing the service characteristics for which the system was designed. The system should also be tested on a regular basis to guarantee that these requirements are being maintained.

Redundancy

The system should be designed with redundancy and backups to help build and maintain a more survivable system. Specific areas requiring redundancy are described below.

- Redundant communications devices (such as modems), surge suppressors, and power supplies [such as uninterruptible power supplies or generators] should be included.

- The core of most ITS is a database. Given this central role, it is important to maintain a backup of the database. Depending on the application, different classes of backups may be required to ensure that the required restoration time is provided. Preferably, this backup database should run on a different machine with a different architecture and a different operating system. This will help alleviate threats that are architecture- or operating-system dependent. A backup communication infrastructure and a network from a different vendor should also be established.

- A RAID (redundant array of independent disks) should be included to help avoid disk failures. There are several levels of RAIDs; consequently, each system may require a different level of RAID, depending on the requirements.

- The operating systems should be maintained with all of the latest operating system patches for both operating system errors and to close security holes, since potential intruders would look for publicized vulnerabilities first.

Backups of the system should be made on a periodic basis.

- An image of a disk containing the operating system, application, and minimal configuration information should be kept for a rapid restoration or configuration of a faulty or new machine.

- Backups should be made and stored both on-site and off-site. On-site backups allow for efficient restoration. Off-site backups are necessary to avoid catastrophes such as theft, fire, or water damage.

System Configuration

All information systems are susceptible to improper configuration and a false sense of survivability. Once the system is designed and built, it must be operated so as to maintain its survivability properties. Access to the system should be as limited as possible. This implies that identification and authentication should be used to limit access to the system, both at the operating system and application levels. Passwords should be checked for strength, both at creation and periodically during use. They should be checked against dictionary words, combinations of personal information, and should contain numbers or punctuation marks. They should also be at least five characters in length. Passwords could be checked by a password checking program such as Crack. If the application software has its own identification and authentication service, it should be utilized with user identifications and passwords different than the operating system user identification and passwords. Email addresses should be different than user identifications so that email, sent on public networks, does not give away the user identification piece of the puzzle. All external connections into the system should have user identification and authentication. All external access should use software that maintains integrity; a specific example is using a secure shell instead of telnet access to the system. Trust relationships (i.e., where you assume that there is no threat of attack or misuse) between machines can weaken the effectiveness of identification and authentication; therefore, trust relationships should not exist. Each change of machine would require users to reauthenticate themselves.

Encryption should be used only for sensitive information. Encryption should generally not be used for data transfer, since the data itself is not very useful. However, commands, such as to change signal timings, should be encrypted to keep intruders from issuing improper commands. Encryption should be done using an established encryption standard and not using a proprietary encryption scheme. This will provide the ability to modify and expand on the system in the future without being forced to retain the original system developer. Along these same lines, all field devices should have a data source authentication mechanism to make sure the commands are coming from the proper authority. One way of authenticating the source of the data is to set up the modems to only perform callbacks. The operator would call the box that would then disconnect, check a list of acceptable numbers, and return the call if and only if the number of the caller was contained in the list of acceptable numbers. Because modems are frequently a weak link in a system, allowing outsiders to gain access to the system without going through protections such as identification and authentication or a firewall, system modems should also be configured for callbacks. Any machine with access to the Internet should be kept completely separate from the other machines, or there should be a firewall that is meticulously maintained between the machine and the other, non-Internet machines. A web server may be set up outside of a firewall such that it receives updates from machines inside the firewall but has no access to any machine inside the firewall.

Principle of Least Privilege

Although identification and authentication are good lines of defense, they cannot be the only lines of defense, since some attackers will get past the identification and authentication protection and other attackers will come from those who already have legitimate inside access to the system. As mentioned, at least fifty percent of intruders are internal (ODS Networks, 1999); hence, the internal attacker (intruder) is certainly a threat. All access to system resources should be configured based on the principle of least privilege. Therefore, the number of personnel with root access should limited. Virus protection software should be used to protect all the machines from malicious codes. Intrusion detection software should be run that can detect external as well as internal intruders. The intrusion detection system, or combination of systems, should contain both anomaly (static and dynamic) and misuse components. Intrusion detection software implies that auditing will need to be performed. However, this auditing is useful in itself for other analysis purposes. To limit access by outsiders, information that is to be shared should be *pushed* to the recipient who is in charge of filtering and processing the information. The outside organization should not have the ability to interact with the system command issuing structure nor should it be able to request data (commonly referred to as *pulling* data). A recovery plan with both physical (redundancy) and policy (procedures to follow) components should be developed and maintained. Along with this plan, there should be a training and awareness program, since people are often the weakest link.

REFERENCES

Anderson, J. P., 1980. Computer Security Threat Monitoring and Surveillance. *James P. Anderson Co. Technical Report*, Fort Washington, PA: Author.

Biesecker, K., Foreman, E., Jones, K., & Staples, B. 1997. Intelligent Transportation Systems (ITS) Information Security Analysis. *United States Department of Transportation Technical Report (*FHWA-JPO Report No. 98-009*)*. Washington, D.C.: Author.

Biesecker, K. & Staples, B. 1997. Protecting Our Transportation Systems: An Information Security Awareness Overview. *United States Department of Transportation Technical Report (*FHWA Report No. JPO-98-005). Washington, D.C.: Author.

Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F. , Longstaff, T., & N.R. Mead. 1997. Survivable Network Systems: An Emerging Discipline. *Carnegie Mellon/Software Engineering Institute* (Technical Report No. CMU/SEI-97-TR-013).

Kemmerer, R.A. 1997. NSTAT: A Model-based Real-time Network Intrusion Detection System. University of California-Santa Barbara (Technical Report No. TRCS97-18), Santa Barbara: Author.

ODS Networks, Inc. (March 1999). Extreme Access . . . Infinite Possibilities. *ODS Networks White Paper*, http://www.ods. com/white/whi 0004.shtml.

President's Commission on Critical Infrastructure Protection. 1997. *Critical Foundations: Protecting America's Infrastructures*. http://www.pccip.gov/report_index.html. Washington, D.C.

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. (May 1998) http://www.whitehouse.gov/WH/EOP/NSC/html/documents /NSCDoc3.html. Washington, D.C.

Ruby, James, King, D., & Gunshol, L., 1997a. State of Maryland Intelligent Transportation Systems Security Requirements Recommendations. United States Department of Transportation (FHWA Technical Report No. JPO-98-013), Washington, D.C.: Author.

Ruby, J., King, D., Gunshol, L., & Hilborn, G. 1997b. State of Maryland Intelligent Transportation Systems Security Implementation Recommendations. United States Department of Transportation (FHWA Technical Report No. JPO-98-014). Washington, D.C.: Author.

Schneier, B. September, (1998, September). Cryptographic Design Vulnerabilities. *IEEE Computer*, pp. 29-33.