Communications security concerns in communications based train control

M. Hartong[1], R. Goel[2] & D. Wijesekera[1]
[1]*George Mason University, USA*
[2]*Howard University, USA*

Abstract

Since the late 1980s, Communication Based Train Control (CBTC) Systems for freight and passenger rail have been under development in the United States. These systems have been advertised as offering significant enhancements in safety by ensuring positive train separation, enforcing speed restrictions, and improving roadway worker protection. In order to maximize the effect of these safety enhancements, it is necessary for CBTC systems to address security issues common to wireless computer communication systems. This paper introduces the role that CBTC systems play in railroad methods of operations, as well as the vulnerabilities of communications systems being manifested in CBTC. It provides a classification of attacks against CBTC systems, and identifies the security controls to mitigate these attacks.

The level of risks associated with these security issues have increased from the first CBTC system introduction, primary because of increases in the means of exploiting the associated vulnerabilities. Exploitation that could compromise the system safety capabilities can take the form of any number of different types of attacks (e.g. jamming, etc). Failure of the CBTC system designer to adequately address these attacks could allow a malicious party to exploit CBTC vulnerabilities, effectively neutralizing the safety advantages of a CBTC system. Recent non-CBTC train-to-train collisions causing release of toxic inhalants and resulting deaths illustrate that a lack of CBTC system safety capabilities could have catastrophic results. Fortunately, these attacks can be mitigated using various security controls. Understanding the attacks and the respective mitigating security mechanisms is therefore key to effectively implementing CBTC safety advantages.

Keywords: security, communications based train control, wireless, communications systems, positive train control.

WIT Transactions on The Built Environment, Vol 88, © 2006 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR060681

1 Introduction

Today's railroads are a critical component in the US transportation and distribution system. US freight railroads have grown in 2003 to a $38 billion dollar industry with 549 freight railroads and 141,000 miles of track. In 2001, the last year for which data has been calculated, that equated to 25% of all intercity freight tonnage carried in the US, and 41% of all ton-miles. This is approximately 12% of all freight revenue in the US in ton-miles, making the rail industry the premier low cost competitive service to other forms of transportation and distribution [1]. Today modern diesel electric locomotives in the US routinely pull over 100 freight cars weighing 286,000 pounds at speeds up to 60 miles per hour. These sizes, speeds, and cargo capacity can result in significantly adverse consequences if the existing methods of train operation fail.

Communication Based Train Control (CBTC) Systems offer protections against the failure of existing methods of train operation. In order to realize these protections, however, it is necessary for CBTC systems to address security issues common to wireless computer communication systems. This paper introduces the role that CBTC systems play in railroad methods of operations, as well as the vulnerabilities of communications systems being manifested in CBTC. It provides a classification of attacks against CBTC systems, and identifies the security controls to mitigate these attacks.

2 Methods of operations and traditional train control

In order to control the movement of trains, various methods of operations began to be formalized starting in the early 1820s when multiple trains began to share the same set of tracks. These methods of operations were designed to improve the operational efficiency and safety of the railroad through the reduction of collisions, derailments, and the associated deaths. Today methods of operations for the control of trains can be classified in to four basic categories: verbal authority, mandatory directives, signal indications, and signal indications supplemented by cab signals, automatic train control, or automatic train stop systems. CBTC systems support these modes of operation.

2.1 Verbal authority and mandatory directives

With verbal authority and mandatory directives, the aspect of wayside signals does not control train operations. Instead, train operations are controlled by orders from the Train Dispatcher, who takes responsibility for knowing what trains are located where, and ensures that no two trains are issued authorization to occupy the same location of track at the same time. The Dispatcher usually issues orders, mandatory directives, speed restrictions, as well as the location of any wayside work crews via two-way radio to the locomotive crew. The train crew then is responsible for ensuring that they obey these orders, speed restrictions, and advisories.

This is the traditional means of controlling operations in the United States, and roughly 40% of all tracks in the United States are controlled in this manner. Verbal Authority and Mandatory Directives operations are generally broken either one of two main types- Track Warrant Control (TWC) and Direct Traffic Control (DTC). TWC and DTC do not require wayside signals. They can, however be used to supplement Automatic Block Signalling (ABS) to increase flexibility and traffic capacity.

When used as a supplemental mode of operation, DTC/TWC serves primarily as a protective overlay to the movement authority and do not convey the authority to occupy the main track. That authority remains with the signal system, but the train crew requires a DTC/TWC authorization in addition to the signal to enter the main track. In TWC the verbal instructions are given for the crew to proceed between stations or mileposts (a segment of track known as the authority limit). DTC is similar to TWC, but because the railroad is divided into pre-defined "blocks." it is simpler in execution. Movement authorities can only be specified in terms of the pre-defined blocks. The decision to use TWC or DTC is made by individual railroads based on what is most efficient for their operations.

2.2 Signal Indications

Train operations under signal indications makes up the remainder of the train control operations in the US. Track circuit based signal systems were first installed in the US in 1872, and in 1927 were centrally controlled in the first "Centralized Traffic Control (CTC)" system. CTC is not a separate control system—it uses block signal system and interlocking to control train movements (although radio communications between the dispatcher and train crews are available).

CTC, sometimes called Traffic Control System (TCS) has remained basically unchanged since the 1930s. In CTC authority for train movements are provided by signal indications. The train dispatcher at the control centre determines train routes and priorities, and then remotely operates switches and signals to direct the movement of trains. The CTC system is designed so that the dispatcher cannot grant conflicting authorities.

Some CTC systems have been enhanced to provide direct indications of wayside signals aspects to the locomotive engineer inside the locomotive cab. These "cab signal" systems provide on-board display of trackside signal indications through the transmission of signal aspect information in coded pulses along the track. The engineer controls the speed of the train with the signal information, and obtains authority to enter sections of track. Further refinements called "automatic train stop" or "automatic train control" systems automatically cause the train to stop or reduce speed where an engineer fails to respond appropriately to a trackside signal.

2.3 Limitations of Current Train Control Technologies

Cab signals simply relay the external signal indications to a visual display inside of the cab of the locomotive, making it easier for the crew to note the signal aspect and the associated order it conveys. Unless operated with ATS or ATC, the cab signal systems do not provide speed or authority enforcement. Consequently, no mechanism would exist to detect and prevent crew non-compliance with dispatcher orders and railroad-operating procedures.

ATS provides enforcement for signal indications. This can be done with or without a cab signals system in place. ATS however, does not provide speed enforcement. It only enforces the indication provided by the wayside signal in the event that the train crew fails to react. ATC, on the other hand, provides both signal indication enforcement as well as speed enforcement.

In general, ATS and ATC systems have several significant technical limitations. First, the location of trains can only be determined to the resolution of the track circuits. The track circuit's length can be made shorter, but adding additional track circuits requires additional wayside hardware. This imposes additional costs, causing a practical (and economical) limit to the number of track circuits that a railroad can install. Second, the information that can be provided to a train through a rail based is limited to a small number of wayside signal aspects or speed data.

In addition, the underlying signal systems to provide the required indications for cab, ATS, or ATC to operate are capital intensive. In 2003, the US Class 1 railroads alone spent over $490 million in operations, administration, and maintenance of all types of communications and signalling systems with another $153 million in deprecation of the existing plant [2] on approximately 65,000 miles of track. Consequently the deployment of these technologies is limited to those areas where rail throughput needs to be maximized. Less than 5% of route-miles in the US [2] have systems in place where signal indications are shown in the locomotive cab or there is on-board enforcement of the signal indications, or both.

3 Communications Based Train Control (CBTC) and methods of operation

Positive Train Control (PTC) is a name applied to select CBTC systems capable of supporting, at a minimum, the following three functions [3]

(a) Prevention of train-to-train collisions (positive train separation).

(b) Enforcement of speed restrictions, including civil engineering restrictions and temporary slow orders.

(c) Protection for roadway workers and their equipment operating under specific authorities.

The inability of cab signals, ATS, and ATC to effectively incorporate collision and accident avoidance measures with the current methods of operations has been the primary motivation for the US National Transportation Safety Board (NTSB) call for PTC [4]. These CBTC systems can overcome the fundamental limitations of conventional ATS and ATC Systems.

In addition to classification by functionality, PTC systems are also classified by the extent that they used to augment the existing method of railroad operations. "Full" PTC Systems do not simply augment the existing mode of operation with their functionality, but change or replace it. “Overlay” PTC systems provide their functionality while maintaining the existing method of operation.

3.1 Generic architecture

The generic PTC functional architecture consists of three major functional subsystems. These are:

(a) The wayside units, consisting of elements such as such as highway grade crossing signals, switches and interlocks or maintenance of way workers,
(b) The mobile units, which are the locomotives or other on rail equipment with their onboard computer and location systems, and
(c) The central office dispatch/control unit.

All of the subsystems are interconnected by communications links.

Each major functional subsystem is a set of physical components implemented using various databases, data communications systems, and information processing equipment. The physical components that make up each subsystem depend upon the functional capabilities of each subsystem. Varying degrees of subsystem functional capability can result in significantly different hardware and software equipment & configurations.

4 CBTC system vulnerabilities

Recent research has examined security and possible problems in the rail infrastructure [5] and surveyed systems in use [6]. Completion of recent regulatory initiatives [7], coupled with accelerated industry efforts in the deployment of CBTC systems [8], have increased the level of risk that the public may potentially be exposed to as a result of the greater use of wireless technology. The most significant source of risk in wireless networks is that the technology’s underlying communications medium, the airwave, is open to intruders.

Changes in malicious hacker activity have shifted from conventional fixed wired systems to wireless networks. These networks have included not only traditional telecommunications systems, but also industrial control systems. Studies by the National Research Council and the National Security Telecommunications Advisory Committee [9] show that hacker activity includes the ability to break into wireless networks resulting in the degradation or disruption of system availability. A recent General Accountability Office study [10] has indicated that successful attacks against control systems have occurred. While these studies were unable to reach a conclusion about the degree of threat or risk, they uniformly emphasize the ability of hackers to cause serious damage.

The resources available to potential intruders are significant [11]. Intelligence is already widely available on the Internet that enables intruders to penetrate any sort of traditional computer network and wireless systems. Detailed vulnerability information is publicly discussed on newsgroups. Tutorials are available that describe how to write automated programs that exploit wireless systems vulnerabilities. Large numbers of automated software tools have been written that enable anyone to launch these types of attacks. Publicly available Web sites whose sole purpose is to distribute this data have been established, often ensuring wide spread distribution of the information before public access can be terminated.

4.1 Attacks

The Information Assurance Technical Framework Forum (IATFF), an organization sponsored by the National Security Agency (NSA) to support technical interchanges among U.S. industry, U.S. academic institutions, and U.S. government agencies on the topic of information assurance, has defined five general classes of information assurance attacks- passive, active, close-in, insider, and distribution [12]

4.1.1 Passive attacks

The danger of a passive attack is a result of the surreptitious way information is gathered. It is the easiest type of attack to execute, and the hardest to defend against. Since the attacker is not actively transmitting or disturbing the transmitted signal of the signal owner, the signal owner (defender) has no means of knowing that their transmission has been intercepted. This kind of attack is particularly easy for two reasons: 1) frequently confidentiality features of wireless technology are not even enabled, and 2) because of the numerous vulnerabilities in the wireless technology security, determined adversaries can compromise the system.

4.1.2 Active attacks

Active attacks that can be launched against a wireless network come from a broad continuum. In its simplest form, active attacks use some mechanism disabling the entire communications channel between the sender and the receiver. With the original sender and receiver unable to recognize transmissions between each other, they cannot exchange information, and are unable to communicate. No detailed knowledge of the message parameters between sender and receiver is required, only a device capable of blocking communications operating over the entire channel.

More sophisticated forms of active attack are the “Denial of Service (DOS)” or the more advanced “Distributed Denial of Service (DDOS). The DOS and the DDOS differ primarily in the location of the origin of the attacks. The DOS originates from only one location, the DDOS from multiple locations. The specific mechanisms of a DOS and DDOS are very communications protocol and product implementation dependent, since these attacks exploit weaknesses in both the communications protocol and the products implementation of the protocol.

Other active attacks are based on exploitation attempts associated with the sender (identity theft, where an unauthorized user adopts the identity of a valid sender), weakness associated with the receiver (malicious association, where unsuspecting sender is tricked into believing that a communications session has been established with a valid receiver,), or weaknesses associated with the communications path (man in the middle, where the attacker emulates the authorized receiver for the sender- the malicious assertion, and emulates the authorized transmitter for the authorized sender- identity theft.). These attacks are primarily geared at disrupting integrity in the form of user authentication (assurance the parties who they say they are), data origin authentication (assurance the data came from where it said it did), and data integrity (assurance that the data has not been changed).

4.1.3 Close in, insider and distribution attacks

These three categories describe the nature of system access, as opposed to the passive or active nature of the attack. Close-in, insider, and distribution attacks make use of some form of either an active or passive attack whose effectiveness is enhanced by the degree of the attackers' access to the system. Insider and distribution attackers usually will utilize their specialized knowledge or access to carry out some form of a passive or active attack.

4.2 Attack mitigation

The basic security mitigations for information and information processing systems attacks in the United States have been codified in law [13]. Specifically these are confidentiality, integrity, and availability. Confidentiality is concerned with ensuring that the data and system are not disclosed to unauthorized individuals, processes, or systems. Integrity ensures that data is preserved in regard to its meaning, completeness, consistency, intended use, and correlation to its representation. Availability assures that there is timely and uninterrupted access to the information and the system.

Closely related to these three are authenticity, accountability, and identification. Authenticity is the ability to verify that a user or process that is attempting to access information or a service is who they claim to be. Accountability enables events to be recreated and traced to entities responsible for their actions. Authenticity and accountability require the ability to uniquely identify a particular entity or process, as well as the authorizations (privileges) that are assigned to that entity. Identification is the specification of a unique identifier to each user or process.

4.2.1 Countermeasures for passive attacks

In general, the preferred mitigation methods for passive attacks are access control and confidentiality. Access control mechanisms are used to prevent unauthorized users accessing services and resources for which they have not been granted permission and privileges as specified by a security policy. Confidentiality can prevent the gain of information about from the content of the messages exchanged.

4.2.2 Countermeasures for active attacks

In general, the preferred mitigation methods against active attack include access control, availability, accountability, authentication, and integrity. The access control and availability countermeasures must maintain or improve data availability. The system must be able to ensure the availability of both data and services to all components in the system. In the event that a PTC platform cannot handle its computational and communication load, it must provide graceful degradation of services and notify the operator that it can no longer provide the level and quality of service expected to prevent an unintentional denial of service.

Ensuring integrity (and confidentiality) places restraints on availability and has performance costs. Encrypting agents and messages in transit may impose unacceptable delays in environments where near real-time response is required.

The use of Cyclic Redundancy Codes (CRCs) is sometimes claimed as a means of providing data integrity. A CRC does not provide protection malicious errors. This is the result of the CRC many to one relationship between its input and output. It is possible for multiple inputs to check sum to a single CRC value. As a result a data substitution can be made, with a correct CRC, and remain undetected. A cryptographic hash functions, where there is a unique one to one relationship between input and output, and where only one data input can check sum to one hash value. Any change in the input results in a change in the hash value, which is detected at the receiver when the hash calculation is carried out and the received hash value does not correspond to the calculated hash value. [14]

Authentication mechanisms provide accountability for user actions. User authentication and data origin authentication differ in that user authentication involves corroboration of the identity of the originator in real time, while data origin authentication involves corroboration of the source of the data (and provides no timeliness guarantees). User authentication methods range from so called time invariant "weak" authentication methods such as simple passwords to time variant "strong" cryptographically based authentication methods. In non-hostile environments no or weak user authentication may be acceptable, while in hostile environments strong user authentication is essential to provide authenticity. Data origin authentication provides assurances regarding both integrity and authentication. They rely on the use of digital signatures and can be either symmetrical or asymmetrical digital signature methods.

5 Summary and future work

This paper has introduced the basic architectures of Positive Train Control. It has highlighted key security issues associated with wireless PTC, and identified the main security requirements that PTC systems must posses. It has also introduced the network security requirements for PTC systems and highlighted basic security interoperability issues.

There are significant areas remaining for future study. Additional work needs to be undertaken to detail the various security architecture requirements of PTC with possible alternative techniques and technologies. The entire area of security network management for PTC systems requires further study, in terms of both policy and technology. Potential interoperability policy and technical issues represents an additional field for further study.

Basic PTC systems, although they are economically unviable in terms of their safety case alone [5, 15], may, when combined with other advanced technologies, potentially offer significant societal benefits [16]. This success, however, will depend, upon the ability to rely on the transmitted information, which will be a function of the security that can be provided.

References

[1] Association of American Railroads, Policy & Economics Department, US Freight Railroad Statistics, 28 October 2004

[2] US Surface Transportation Board, Office of Economics, Environmental Analysis and Administration "Statistics of Class I Freight Railroads in the United States 2003"

[3] Federal Railroad Administration Railroad Communications and Train Control Report to Congress, July 1994

[4] US National Transportation Safety Board, "NTSB Most Wanted Transportation Safety Improvements 2004-2005", November 2004

[5] Carlson, Frincke, Laude, "Railway Security Issues: A Survey of Developing Railway Technology", Proceedings of the International Conference on Computer, Communications, & Control Technology, International Institute of Informatics and Systematics, 2003.

[6] Craven, "A Brief Look at Railroad Communication Vulnerabilities", Proceedings 2004 IEEE Intelligent Transportation Systems Conference Washington, D.C

[7] National Archives and Records Administration, "49 CFR Parts 209, 234, and 236 Standards for the Development and Use of Processor Based Signal and Train Control Systems; Final Rule", Federal Register, 7 March 2005

[8] National Transportation Safety Board Positive Train Control Systems Symposium March 2-3, 2005 Ashburn, Virginia http://www.ntsb.gov/events/symp_ptc/symp_ptc.htm

[9] The President's National Security Telecommunications Advisory Committee Wireless Task Force Report "Wireless Security" January 2003

[10] United States General Accountability Office, GAO Testimony Before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems", Tuesday, March 30, 2004

[11] Investigative Research for Infrastructure Assurance Group, "Diversification Of Cyber Threats", Institute For Security Technology Studies At Dartmouth College, May 2002

[12] US National Security Agency Information Assurance Solutions, Fort Meade, MD, "Information Assurance Technical Framework (IATF), Release 3.1, Sept 2002, ,

[13] Federal Information Security Management Act of 2002 (Public Law 107-347) December 2002.

[14] Menezes, van Oorschot, Vanstone, "Handbook of Applied Cryptography" 5ed, CRC Press, Aug 2001

[15] Federal Railroad Administration, "Report of the Railroad Safety Advisory Committee to the Federal Railroad Administrator, Implementation of Positive Train Control Systems" August 1999

[16] Federal Railroad Administration, "Benefits and Costs of Positive Train Control, Report in Response to Request of Appropriations Committees", August 2004