Evaluating Cyber Attacks in Rail Transit

Manoj K. Jha
Morgan State University, USA

Ronald A. Keele
Morgan State University, USA

INTRODUCTION

It is 1:00 a.m.; he just awoke from his late night nap. Dubbed "Da_Terminator;" this Black Hat hacker is about to break into one of the most sophisticated computer systems outside of the Federal Government. That system is commonly known as the Train Control System (TCS) of your local Rail Transit Agency (RTA). In response to the September 11th attacks, Rail Agencies across the United States strengthened the physical security around their fixed assets, especially railway bridges and rail maintenance yards but not their computer systems. Given the probability of attacking various rail control systems, it is not hard to imagine these hackers causing all kinds of collisions and derailments that would spill chlorine, nuclear waste and/or a host of other toxic chemicals that travel our railways every day. These incidents would compel authorities to evacuate large neighborhoods, and in some instances, entire towns. In many cases, the casualties could be large, depending on the location of the release and the weather. But if a hacker wanted to go the extra mile, s/he could access the national database that lists authorized railway routes for transporting hazardous materials, and cross-reference that with another database, this one identifying exactly what chemicals are in what railroad cars at any given time. Mix that information with data from another railway scheduling database, add control of the railway switching operations, and a hacker could, theoretically, target trains carrying the most toxic chemicals, causing them to derail and release their cargo in the most populated areas during the worst time of the day; rush hour (Gallagher, 2012)!

Due to the increasing complexity of these new software-driven systems and the total reliance on these same systems to improve safety; evaluating cyber attack scenarios, along with the analysis of cost interruptions, can reduce the system's risk in the event of a software malfunction. It is the purpose of the chapter to assist those responsible for these systems to also conduct a vulnerability assessment of their system's operations.

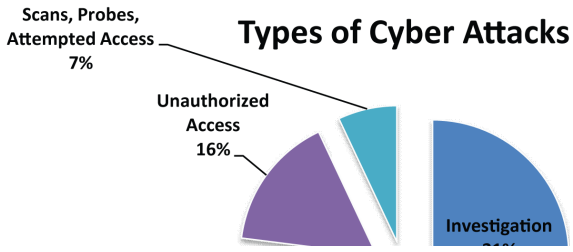
BACKGROUND

Businesses have reported increasing numbers of cyber attacks that have placed sensitive information at risk, with potentially serious impacts on operations, assets, and personnel. Over the past six years, the number of reported incidents has increased from 5,503 incidents in fiscal year 2006 to 42,887 incidents in fiscal year 2011, an increase of almost 680% (Dempsey, 2013). These businesses reported the types of cyber attacks as indicated in Figure 1. The two most prevalent types of attacks reported were the unconfirmed incidents under investigation and malicious code (GAO, 2012).

The above threats are real enough that the National Defense Research Institute (NDRI) cited a rail-related, cyber attack in a report prepared for the U.S. Secretary of Defense. As part of a complex threat scenario, NDRI included "*an Amtrak Acela Express Train traveling at 150 mph slammed into an apparently misrouted freight*

DOI: 10.4018/978-1-4666-5202-6.ch081

Figure 1. Types of cyber attacks reported (GAO, 2012)



train near Laurel, Maryland. The Maryland State Police estimated that the train wreck had killed over 60 passengers and crew and critically injured another 120 persons. Within three hours, the National Transportation Safety Board's (NTSB) Chief Rail Investigator notified the Secretary of Transportation that there was 'clear evidence' that the freight train had been misrouted onto the Acela track with 'some evidence' pointing to a sophisticated intrusion into the East Coast Train Control System."

What is a Train Control System and what does it do, you might ask? It controls a train's movement (forward/reverse movement and train separation/spacing); its track diversions (switches); its signaling systems (go/no go) and the train-to-wayside communication systems (train destination, train number, train length [number of railcars in the train consist], opening/closing of train doors, speed restrictions and station checks). The TCS is the nerve center of the RTA and its primary functions are to; (1.) monitor the performance of the rail system and to display the system's status to the rail controller and (2.) select and exercise the control strategies necessary to regulate the traffic flow to even out and keep the trains separated. The TCS's capabilities include both automatic and interactive control in which the rail controller initiates action based on displayed information. The TCS usually includes a dual computer system with its own software and a control console with high definition (HD) television monitors. Also, provisions have been made for back-up power supply sources so that train operations can be maintained should the normal power supply fail. The HD television monitors display for the rail controller each train route in the form of a schematic track representation (see Figure 2). Each train in the system is displayed on the schematic at its actual location. The representation of each train's position is a train symbol which denotes the direction of travel and the train's destination. The train's route number can be displayed at the rail controller's command. The TCS monitors the entire rail transit system and initiates correction commands to smooth traffic flow. These correction commands can be generated automatically by the computer, but if conditions warrant, the computer alerts the rail controller and informs him/her of the conditions. Corrective action is

Figure 2. A rail controller with a schematic layout of the rail system