IDC HERZLIYA

ICT International Institute for Counter-Terrorism
With the Support of Keren Daniel

ICT Cyber-Desk

Insight

Assessing the Cyber Threat to the Train Industry
April 2016

Assessing the Cyber Threat to the Train Industry[1]

On the morning of February 9, 2016, two trains collided head-on near the city of Bad Aibling, approximately 60 km. from Munich, Germany. Ten people were killed in the crash and dozens more were injured, 18 of them critically. As of this moment, the reasons for the accident have not yet been published and the question remains as to whether it was the result of human error or a defect in one of the systems entrusted to maintain safety and prevent such accidents from occurring.[2] According to several evaluations, one of the safety systems had been disarmed as part of a deliberate act and, as a result, there was no warning of the collision.[3]

Over recent decades we have witnessed several successful attacks and attempts by terrorist organizations to strike trains around the world. Most of these attacks were carried out in Asia and Europe where the rail infrastructure is a common means of transportation. An attack and/or successful threat against train function is liable to disrupt the country's normal activity, damage its economy and even harm people.

Conventional Threats

Over the last decade, several physical terrorist attacks have been successfully carried out on trains in capital cities such as Madrid, London and Ankara, with most of the attacks involving explosives and suicide bombers:

1. In March 2004, a group of radical Islamists influenced by Al-Qaeda carried out a terrorist attack using explosive devices on a train in Madrid. 191 people were killed in this attack and over 1,800 were injured. The attack included a series of ten charges that were activated next to four railroad cars (three other charges that did not explode were discovered after the attack).[4]
2. In July 2005, a cell composed of four Al-Qaeda suicide terrorists carried out a simultaneous attack on several subway stations and a bus in London. Over 50 people were killed in the attack and approximately 700 others were injured.[5]
3. In October 2015, over 100 people were killed and approximately 400 others were injured in

---

[1] *Written by Nir Tordjman and Oren Elimelech.*
[2] http://www.independent.co.uk/news/world/europe/german-train-crash-probe-into-bavaria-crash-focussing-on-human-error-by-signals-controller-a6865191.html
[3] http://www.bbc.com/news/world-europe-35539089
[4] https://www.ict.org.il/Article/1073/The-Madrid-Bombings-and-Global-Jihadism
[5] https://www.ict.org.il/Article/1002/The-Aftermath-of-7-July-New-Trends-in-Terror

two terrorist attacks that were carried out outside of the central train station in Ankara. Even though no organization claimed responsibility for the attack, one of the suicide terrorists was identified as a supporter of the Islamic State.[6]

4. In March 2016, three Islamic State suicide terrorists carried out two terrorist attacks in Brussels, Belgium, about one hour apart, killing 31 people and injuring hundreds more. The first attack took place at the airport and the second attack took place at the metro station.[7]

In addition to threats and physical attacks, the dependency of the rail system on cyberspace makes it a preferred target for terrorist attacks. Terrorist organizations can exploit security weaknesses and loopholes in the computing systems of trains, thereby disrupting their normal and scheduled operation to the point of causing actual damage, be it financial in light of the disrupted activity, or loss of life in the case of a passenger car collision. A successful attack on the online train infrastructure can cause direct and indirect economic damage, as well as disrupt the daily routine of civilians who depend on the proper operation of public transport.

The increased involvement of foreign fighters and supporters in terrorist organizations, who in many cases were raised, educated and worked in Western countries, is likely to influence the attack target selected by terrorists while utilizing prior accumulated knowledge and experience. Examples of this include the explosive charge that was detonated on a plane in Somalia after an airport employee had smuggled the device onto the field and passed it to the terrorist,[8] and the explosive charge that was hidden in a soda can and caused the downing of a passenger airplane in Sinai.[9]

Experience over recent years has shown that there are supporters of terrorist organizations who receive training, information and access to critical systems or restricted areas near their place of work or residence. The danger is that those supporters will become active participants and help to carry out a terrorist attack, either by transmitting information or transferring/planting a bomb at a selected target. The attack in Somalia is only one example that illustrates just how easy it is to breach security at an airport with help from an employee "on the inside".

---

[6] https://www.ict.org.il/Article/1552/Saudi-Arabia-Announced-a-New-Military-Alliance-to-Fight-terrorism
[7] https://www.ict.org.il/Article/1645/The-Brussels-Attacks
[8] http://www.foxnews.com/world/2016/02/07/investigators-find-video-possible-somalia-bomb-handoff.html
[9] https://www.ict.org.il/Article/1521/ISIS-close-to-home

A similar incident could also take place in the train industry in the future, as trains are also considered part of a country's critical infrastructure. It is likely that there are activists or supporters who are working either directly or indirectly in the rail system, and are proficient in the operating systems, methods and procedures of trains, and are familiar with their existing weaknesses. These activists could use cyberspace, among other means, to sabotage and manipulate the control systems, which would cause damage to infrastructure or to human life.

In December 2015, several prolonged blackouts occurred in Ukraine. The disabling of the electricity systems in Ukraine was carried out through a cyber-attack using the BlackEnergy crimeware that attacked SCADA systems, and through the deletion of systems using KillDisk, which caused all of the systems to become inactive. The company, TrendMicro, recently reported that it had discovered traces of BlackEnergy and of KillDisk in one of the systems of the major railway operators in the country.[10]

Cyber Threats

Cyberspace serves as a wide arena of activity with points of weakness that can cause the disruption of normal functioning and even result in human casualties. Passenger trains are operated and administered by a range of electronic management and control systems, some of which are remotely operated and controlled. These systems are also under scrutiny in order to identify security weaknesses and vulnerabilities. A group that answers to the name "StrangeLove SCADA"[11] published[12] the results of an extensive, three-year study, which found a large number of weaknesses that influence the signal and control systems of trains and support systems for rail-related activities. The study was carried out by two information-security researchers, Alexander Timorin and Sergei Gordeychik, who received training as a train automation engineer. The researchers found that train systems are usually not connected to the Internet but security breaches of equipment and systems allow potential attackers to exploit these points of weakness in order to penetrate the system as a first step in carrying out an attack on the railway system by disrupting the capabilities of the command and control systems.

[10] http://securityaffairs.co/wordpress/44452/hacking/blackenergy-mining-and-railway-systems.html
[11] http://scadastrangelove.org/
[12] http://www.slideshare.net/AlexanderTimorin/the-great-train-cyber-robbery-scadastrangelove

The concern raised by the researchers is that systems that used to be manual, such as the Signaling System, have mostly become automatic today. In addition, the researchers noted that engineering systems and entertainment systems usually share the same communication network – poor planning that can lead to vulnerability and exploitation.

The study does not address specific trains and does not provide precise information in order not to expose points of weakness and vulnerability, but it does list the problems found in the train systems in general. The study provides information about the EuroStar train, which connects England, France and Belgium. This train uses seven different automation systems, some of which are susceptible to unauthorized remote access, as well as to manipulation by hostile elements. Among the weaknesses that were discovered in this system, the researchers noted: a lack of basic protection on the authentication level (user identification process) that does not exist in old protocols and operating systems, passwords that are hard-coded for the sake of remote control and connectivity, and more.

Among the systems that had weaknesses revealed, according to the study, were a protection system used in most European countries. This system performs a computer-based automation process for various train components. Sibas systems are susceptible because they use WinAC RTX, the Siemens SIMATIC software controller, a Programmable logic controller (PLC) previously recognized as vulnerable by the researchers. Other Computer-based Interlocking (CBI) systems, which are used in most train companies, are also susceptible. CBI elements are used to command and control train routes and are essential for streamlining train movement operations and preventing collisions.

The researchers even noted that attackers could bring down these systems, trigger their complete shutdown, or cause an accident that could result in serious physical injury, economic damage and more. In order to carry out such an attack, physical access to the systems is necessary or, alternatively, the ability to recruit employees from the inside. It is also possible to trick employees with deceptive phishing-type attacks or through a USB connection to a network component through which they can sabotage the system.

Another potential point of weakness is through the use of GSM-R SIM cards, which are used primarily for tracking the movement of trains in several countries in the world, but are also used to manage operations and certain commands, including sending the stop command to the train when

necessary. The research group discovered that trains stopped automatically when the connection was lost between the SIM and the central control and command system, even in the case of GSM frequency jamming. It was discovered that the original code of some of the cards, which were set at default, had never been changed by the train staff. In addition, modem devices that use the SIM cards allow firmware upgrades OTA (over-the-air), which enables it to be hijacked by a skilled attacker. In addition, some GSM-R compatible modems were found to be susceptible to mobile modem attacks, which were already reported several weeks ago in another article released by the researcher group.

In summary, while the researchers claim that even though advanced knowledge of ICS/SCADA systems is necessary in order to implement this kind of attack, world powers/countries or even financing/assistance players from the government are capable of investigating the issue and achieving the operational maturity necessary for an attack. There are terrorist organizations that receive assistance, training and instruction from states, which improves their operative capability in cyberspace. Other terrorist organizations, such as the Islamic State, absorb into its ranks members with expertise and experience in carrying out cyber-attacks.

The exposure and publication of these security weaknesses are designed to motivate decision makers to work quickly to find solutions to the security breaches discussed. It can be assumed that the publication of these weaknesses is also liable to increase the motivation of terrorists to try and carry out a cyber-attack, especially those with advanced expertise in train infrastructure.

ABOUT THE ICT

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy. ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

ABOUT ICT CYBER-DESK

The Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse); and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack). The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations.

Click here for a list of online the ICT Cyber-Desk publications

For tailored research please contact us at Webmaster@ict.org.il.