Transportation Cybersecurity Incidents

THE UNIVERSITY OF ALABAMA | Alabama Transportation Institute

Overview

Modern transportation networks are systems of systems, combining traditional information technology and real-time operational technology with a goal of producing seamless, efficient mobility. However, the more technology is integrated into every mode and aspect of transportation, the greater the risk and the potential for disruption, with consequences ranging from inconvenience to large-scale loss of life. A great need exists to protect electronic, digital, radio, and automated aspects of systems from malicious acts. The response to this need is generally referred to as cybersecurity. The purpose of this report is to demonstrate the breadth of recent threats by providing a summary of open-source reported vulnerabilities and attacks in the transportation domain.

2010

- Researchers at the University of California – San Diego and the University of Washington demonstrated:[1]
  - Vehicles can be completely compromised via physical access to Bluetooth, the media player, diagnostics port and/or cellular.
  - Telemetric capabilities can be used to gain access and compromise various cars.
  - One attack was done simply by calling the car.
- Using $1500 in equipment, researchers at the University of South Carolina and Rutgers University successfully compromised tire-pressure monitoring systems (TPMS) and were able to track a vehicle's location and provide false tire pressure readings.[2] This act proved access to systems is attainable without physical access to the vehicle.

2011

- In August 2011, a cyber-attack on Iranian Shipping Lines caused weeks of disorder and significant financial loss.[3]
- Iran claimed it caused a highly classified drone to land in Iran rather than its target by "fooling" the GPS.[4]
- A French researcher was able to capture vehicle to vehicle communication via remote sniffing stations, allowing very good accuracy in terms of pinpointing passenger location.[5]

2012

- A DARPA funded effort demonstrated vulnerabilities in 2010 Ford Escape and 2010 Toyota Prius model vehicles. Functions such as power steering and GPS were disabled by flooding them with arbitrary CAN packets.[6]
- A disgruntled employee at a Texas automotive dealership broke into the company's system and activated a vehicle immobilization system that shut down over 100 cars.[7]
- The University of California – San Diego demonstrated an attack into a dealership system, planting malware on vehicle diagnostic tools. Whenever a vehicle was connected to the tools, the malware jumped to the vehicle.[8]
- Thieves in the UK targeted BMWs with a multitier cyber attack. They sat with RF jammers near cars and block the remote locking signal sent from the user's key fob to the car, essentially leaving the car open. They would then enter the car, plug a device into the car's OBD-II connector, program a blank fob, and drive off with the car.[9]
- University of Texas-Austin researchers spoofed the GPS of a helicopter drone, almost forcing it to crash.[10]
- It was revealed that a major cyber operation dubbed "Red October" had been ongoing since 2007, and had targeted energy providers, nuclear sites, and critical infrastructure.[11]
- The Shamoon virus was used to attack oil refineries in Saudi Arabia and Qatar. This forced Saudi Aramco to go offline, caused major operational issues, including the production of crude oil.[12]
- A piece of malware called Wiper was used to erase information off the hard drives of Iranian oil companies.[13]

2013

- Organized crime hacked into cargo systems in Australia and the Netherlands to ensure delivery of illicit goods.[14]
- Researchers used a $3,000 GPS spoofer to steer an $80 million yacht off course.[15]

2014

- Cybercriminals forged a fuel supply tender to fool the World Fuel Service, and subsequently took delivery of $18 million worth of marine gas and oil.[16]
- A DARPA study that reviewed 21 different model vehicles concluded:[17]
  - Bluetooth is one of the most viable and largest attack points;
  - In-car apps and web browser technology present a significant risk due to deep understanding/experience of these type of interfaces by attackers.
- University of Michigan researchers hacked into nearly 100 wireless networked traffic lights, and were able to change their state on command. They also found means to hack road signs to change the output. The overall effort was deemed as "easy."[18]

2015

- The British rail network was attacked four times in 2015.[19]
- A Massachusetts Bay Transportation Authority train traveled five stations without an operator controlling it. Though never confirmed, a cyber attack was widely hypothesized.[20]
- According to a report produced by IBM, automotive manufacturing accounted for almost 30% of the total cyber attacks against the manufacturing industry in 2015.[21]

2016

- Researchers at the University of South Carolina, Zhejiang University, and the Chinese security firm Qihoo 360 demonstrated they could jam various sensors on the Tesla S, making objects invisible to the navigation system.[22]
- A French researcher was able to hack the lidar systems on self driving cars so as to trick the sensor into thinking objects were there when they were not, and vice versa.[23]
- A research study showed that the geo-positioning cards used on British trains are prone to mobile attacks via the modem, and that many times the default password to the devices (1234) is never changed.[24]
- A Thanksgiving weekend ransomware attack on the San Francisco light rail system infected a substantial amount of the system, causing varying degrees of damage.[25] The attack's consequences were significant enough that passengers rode free for the weekend due to technical challenges.[26]
- There were multiple attacks against metro and train control systems in South Korea.[27]
- Vietnam Airlines and the two largest airports in Vietnam were the target of cyber attacks. The attacks affected check-ins, flight information screens, website content, and even the speaker system for the airport, which was used to spread propaganda. The attack caused flight delays.[28]
- The Perth Airport in Australia was hit with a cyber-attack, in which they lost a significant amount of data.[29]
- In a three year study by IOActive, half of known vehicle vulnerabilities would allow attackers to take control, and 71% are easy to exploit. The report suggests some of the vulnerabilities are "insecure by design."[30]

2017

- The NotPetya worm disrupted shipping giant Maersk's operations for over two weeks, costing an estimated $300 million in losses.[31]
  - The incident forced the shutdown of the largest cargo terminal at the Port of Los Angeles.
  - Maersk employees resorted to using Twitter, WhatsApp and Post-It notes as workarounds to move cargo from ship to shore.
- A medium sized shipping firm in the UK was attacked so that emailed bills from fuel suppliers were modified to list the attacker's bank account as the payment stop, costing the firm several million dollars.[32]
- Pirates hacked into a major shipper's systems to determine which ships were carrying cargo they wanted to seize. Upon boarding the ships, they used the barcode on the containers to find and take only the desired cargo.[33]
- An unknown party manipulated GPS signals in the eastern part of the Black Sea, leaving approximately 20 ships with no situational awareness, and reporting that other ships in the area were actual inland near an airport.[34]
- A distributed denial of service attack hit Sweden's transportation network, causing delays, crashing the IT system that monitors train location and taking down the email server.[35]
- The US Navy investigated whether a cyber-attack caused the USS John McCain and a tanker to collide.[36]

2017 (continued)

- Security researchers hypothesized a scenario in which attackers could manipulate the loading data of a ship's hull stress monitoring system to deliberately imbalance the cargo, causing the vessel to sink.[37]
- A cybersecurity firm successfully penetrated an operating system controlling a vessel's navigation, radar, pumps, and machinery (ECDIS) and:[38]
  - Shifted the vessel's reported position,
  - Misled the radar,
  - Caused machinery to be disabled,
  - Caused signals to fuel and ballast pumps to be overridden, and
  - Gained control of steering.
- FedEx announced that worldwide operation of its TNT Express unit was hit with the NotPetya worm, causing an estimated $300 million in losses.[39]
- Hackers attacked Germany's Deutsche Bahn. Train departure boards showing ransom demands.[40]
- UK and German officials set up a mythical/virtual rail transport control system honeypot to better gauge attackers frequency and capabilities.[41]
  - In six weeks, 2,745,267 attack attempts were recorded.
  - Over 40% of the attacks originated in China .
  - Attackers succeeded four times in logging into the system.
  - Security configuration of an industrial control was compromised, allowing a physical effect.
  - Attackers also successfully penetrated the media server, which allowed access to the website.
- The Sacramento Regional Transit was hit with a cyber attack.[42]
- Ukraine's Odessa airport was hit with a ransomware attack, causing flight delays.[43]
- Kiev's metro system's payment system was attacked.[44]
- Attackers took over a fleet of autonomous delivery trucks, rerouting them all to Manhattan at 3 mph. This caused major gridlock in the city.[45]
- Attackers sent a message to London's Heathrow Airport stating that they had compromised the baggage handling system and would take it down if not given $1 million. They also indicated they would prove this capability at a given time. The airport authorities complied rather than having the system go down.[46]
- Renault, Nissan, and Honda were forced to temporarily shut down assembly plants due to the Wannacry virus.[47]
- Researchers at Trend Micro published a report indicating how a fundamental security issue in the CAN protocol would allow attackers to shut off a car's key automated components, including safety systems, via a denial of service attack. This includes airbags, anti-lock brakes, and door locks. The attack has been shown to foil the few vehicle-based intrusion detection systems on the market.[48]
- Days before the 2017 Presidential Inauguration, a cyber attack took control of 70% of 187 Washington D.C. traffic and security cameras and held them for ransom. No ransom was paid and arrests were made.[49]

2018

- An attack based in China hacked operators, defense contractors, and telecommunications companies involved with US satellites, gaining access to control positioning and disrupt data traffic.[50]
- Danske Statsbaner (the largest Danish train operating company) was hit with a massive denial of service attack that stopped all ticket purchases via electronic means.[51]
- Suburtan Toronto transit authority Metrolinx was hit with a malware attack attributed to North Korea.[52]
- A ransomware attack hit Baltimore's 911 systems causing a 17 hour shutdown.[53]
- A cyber-attack on Atlanta's municipal government basically shut down many municipal functions for several days, and workarounds continued for many weeks.[54]
- The Colorado Department of Transportation was hit twice with ransomware attacks within a month.[55]
- Mecklenburg County, North Carolina (Charlotte) had to rebuild its entire IT system after a ransomware attack. It took over 60 days to return to normal.[56]
- A 2018 report highlighted 112 billion bot requests and 3.9 billion malicious login attempts against systems belonging to airlines, cruise lines, hotels, online travel, automotive rental and transport organizations.[57]
- Nearly a quarter of United Kingdom manufacturers claimed they suffered losses due to cyber attacks.[58]

[1] https://venturebeat.com/2016/06/27/the-5-scariest-car-hacks-including-some-that-could-make-you-crash/
[2] https://venturebeat.com/2016/06/27/the-5-scariest-car-hacks-including-some-that-could-make-you-crash/
[3] https://www.csoonline.com/article/3245803/security/defeating-21st-century-pirates-the-maritime-industry-and-cyberattacks.html
[4] https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation
[5] http://www.businessinsider.com/driverless-cars-hacking-ricks-2016-12
[6] https://venturebeat.com/2016/06/27/the-5-scariest-car-hacks-including-some-that-could-make-you-crash/
[7] https://www.computerworld.com/article/2505402/security0/car-hacking--remote-access-and-other-security-issues.html
[8] https://www.computerworld.com/article/2505402/security0/car-hacking--remote-access-and-other-security-issues.html?page=2
[9] https://www.computerworld.com/article/2505402/security0/car-hacking--remote-access-and-other-security-issues.html?page=2
[10] https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation
[11] https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm
[12] https://en.wikipedia.org/wiki/Shamoon
[13] https://en.wikipedia.org/wiki/Wiper_(malware)
[14] https://www.csoonline.com/article/3245803/security/defeating-21st-century-pirates-the-maritime-industry-and-cyberattacks.html
[15] https://www.csoonline.com/article/3218724/security/navy-considering-possibility-of-cyberattack-after-another-ship-collision.html
[16] https://www.csoonline.com/article/3245803/security/defeating-21st-century-pirates-the-maritime-industry-and-cyberattacks.html
[17] https://venturebeat.com/2016/06/27/the-5-scariest-car-hacks-including-some-that-could-make-you-crash/
[18] https://www.csoonline.com/article/2466551/microsoft-subnet/hacking-traffic-lights-with-a-laptop-is-easy.html
[19] https://www.sentryo.net/cyber-security-trains-firing-line-of-hackers/
[20] https://www.securityweek.com/why-mass-transit-could-be-next-big-target-cyber-attacks%E2%80%94and-what-do-about-it
[21] https://www.darkreading.com/vulnerabilities---threats/manufacturers-suffer-increase-in-cyberattacks/d/d-id/1325209
[22] https://www.technologyreview.com/s/608618/hackers-are-the-real-obstacle-for-self-driving-vehicles/
[23] http://www.businessinsider.com/driverless-cars-hacking-ricks-2016-12
[24] https://www.sentryo.net/cyber-security-trains-firing-line-of-hackers/
[25] https://www.cnbc.com/2016/11/28/cybersecurity-experts-.html
[26] https://www.securityweek.com/why-mass-transit-could-be-next-big-target-cyber-attacks%E2%80%94and-what-do-about-it
[27] https://www.securityweek.com/why-mass-transit-could-be-next-big-target-cyber-attacks%E2%80%94and-what-do-about-it
[28] https://en.wikipedia.org/wiki/Vietnamese_airports_hackings
[29] https://www.tripwire.com/state-of-security/latest-security-news/criminal-stole-a-significant-amount-of-data-in-airport-hacking-attack/
[30] https://www.computerweekly.com/news/450302150/Half-of-vehicle-cyber-vulnerabilities-could-give-hacker-control-study-shows[30]
[31] http://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html
[32] https://www.bbc.com/news/technology-40685821
[33] https://www.bbc.com/news/technology-40685821
[34] https://www.csoonline.com/article/3218724/security/navy-considering-possibility-of-cyberattack-after-another-ship-collision.html
[35] http://www.transportsecurityworld.com/ddos-attack-cripples-danish-rails-ability-to-sell-tickets
[36] https://www.csoonline.com/article/3218724/security/navy-considering-possibility-of-cyberattack-after-another-ship-collision.html
[37] http://www.seatrade-maritime.com/news/europe/naval-dome-exposes-vessel-operational-vulnerabilities-to-cyber-attack.html
[38] http://www.seatrade-maritime.com/news/europe/naval-dome-exposes-vessel-operational-vulnerabilities-to-cyber-attack.html
[39] http://www.fleetowner.com/technology/cybersecurity-battle
[40] https://www.railengineer.uk/2017/05/30/hacking-the-railway/
[41] https://www.railengineer.uk/2017/05/30/hacking-the-railway/
[42] https://www.sacbee.com/news/local/transportation/article185934933.html
[43] https://www.reuters.com/article/us-ukraine-cyber/new-wave-of-cyber-attacks-hits-russia-other-nations-idUSKBN1CT21F
[44] https://www.reuters.com/article/us-ukraine-cyber/new-wave-of-cyber-attacks-hits-russia-other-nations-idUSKBN1CT21F
[45] https://www.csoonline.com/article/3284349/security/ddos-attacks-on-the-rise-china-and-russia-behind-most-credential-abuse-attacks-report.html
[46] https://www.csoonline.com/article/3284349/security/ddos-attacks-on-the-rise-china-and-russia-behind-most-credential-abuse-attacks-report.html
[47] https://automotivelogistics.media/intelligence/cyber-safety-supply-chain
[48] https://www.wired.com/story/car-hack-shut-down-safety-features/
[49] https://www.cbsnews.com/news/days-before-inauguration-hackers-breached-traffic-security-cameras-around-washington-dc/
[50] https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html
[51] http://www.transportsecurityworld.com/ddos-attack-cripples-danish-rails-ability-to-sell-tickets
[52] https://www.itworldcanada.com/article/ontario-transit-agency-extremely-confident-cyber-attack-came-from-north-korea/401047
[53] https://www.denverpost.com/2018/03/30/cdot-cyberattack-local-government-preparation/
[54] https://www.denverpost.com/2018/03/30/cdot-cyberattack-local-government-preparation/
[55] https://www.denverpost.com/2018/03/30/cdot-cyberattack-local-government-preparation/
[56] https://www.denverpost.com/2018/03/30/cdot-cyberattack-local-government-preparation/
[57] https://www.csoonline.com/article/3284349/security/ddos-attacks-on-the-rise-china-and-russia-behind-most-credential-abuse-attacks-report.html
[58] https://www.infosecurity-magazine.com/news/a-quarter-of-uk-manufacturers/

Acknowledgement

This report was prepared by John Callahan for the Cyber Institute and the Alabama Transportation Institute at the University of Alabama.