PREVENTION AND SECURITY ARCHITECTURE KEEP **TRANSPORTATION ON THE RIGHT TRACK**

Introduction

Improvements to transportation have always been the key for building greater wealth for transportation providers, their customers, and nation states. Consequently, attacks on transportation originate from criminals as well as state-sponsored threat actors and terrorist groups.

Today's advances derive from the digital transformation. The Covid-19 pandemic has accelerated migration to digital technology by 5 [1] to 6 [2] years. However, transportation's growing use of connected compute power has also made transportation subject to increasingly sophisticated cyber attacks from criminals and government-sponsored advanced persistent threat (ATP) groups. This paper examines how adding digital technology calls for a reevaluation of cyber security.

[1] John Koetsier, 97% Of Executives Say Covid-19 Sped Up Digital Transformation, Forbes, Sep 10, 2020. https://www.forbes.com/sites/johnkoetsier/2020/09/10/97-of-executives-say-covid-19-sped-up-digital-transformation/?sh=278883384799

[2] Michele Grover, COVID-19 has sped up digital transformation by 5.3 years, says study, IoR Now, Anasia D'mello - July 23, 2020.

How Transportation is Digitally Transforming

ICS and OT are merging with the Internet

Industrial Control Systems (ICS) manage, direct, and regulate industrial devices and systems. Highway, surface transportation, aviation, maritime, and especially pipeline providers are increasingly dependent on ICS for operations and safety.[3] Previously, standalone ICS and operating technologies (OT) have been hard to attack as bad actors had to introduce malware manually via a disc or an infected USB device. The integration of ICS and OT with the Internet has made ICS and OT vulnerable to multi-vector cyberattacks launched from the Internet. Making matters worse, legacy ICS and OT software often contains software vulnerabilities for which manufacturers don't now or never did provide patches. It is important for transportation providers to have purpose-engineered security controls for their ICS and OT systems including those using SCADA protocol.

AI and autonomous cargo vehicles on land, sea, and air

The pandemic is stranding maritime crews and cargo truck drivers as well as grounding air fleets due to quarantines and travel restrictions. In addition to the problem of human availability, human error is a major caused of accidents and safety issues. According to an Allianz study, human error is responsible for between 75% and 96% of marine casualties.[4] Likewise, exhaustion is a factor in about 14% of fatal truck accidents.[5] To solve this, the race is on to replace human-operated vehicles with autonomous vehicles guided by artificial intelligence (AI). AI never gets tired, doesn't get distracted, and isn't subject to human illness. Maritime Autonomous Surface Ships (MASS), autonomous cargo trucks, and autonomous commercial aircraft[6] are rapidly becoming the solution for safety and human availability issues.

However, autonomous and connected vehicles are tempting targets for cyber attacks due to the growing variety of software and communication interfaces which increases complexity and connectivity,[7] both enemies of cyber security. As autonomous vehicles come online, they must be protected from cyber attacks to prevent thefts, data breaches, sabotage, and other damage.

---

[3] Lisa Kaiser, Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy 2013-2023, Department of Homeland Security.

[4] Prableen Bajpai, Autonomous Shipping: Trends And Innovators In A Growing Industry, Nasdaq, February 18, 2020, https://www.nasdaq.com/articles/autonomous-shipping%3A-trends-and-innovators-in-a-growing-industry-2020-02-18

[5] Katie Myers, Self-Driving Semi-Trucks: Who, What, When, and Why — Part 1, Flockfreight, March 10, 2020. https://www.flockfreight.com/2020/03/10/self-driving-semi-trucks-who-what-when-and-why-part-1/

[6] For an example see Elroy Air as viewed December 18, 2020. http://www.elroyair.com/

[7] For an example see Elroy Air as viewed December 18, 2020. http://www.elroyair.com/

GPS systems

On July 23, 2020, a Russian cyber crime group called EvilCorp attacked GPS maker Garmin. The attack disrupted many critical aviation systems responsible for navigation, autopilots, active traffic systems, flight instruments, engine information systems, displays, sensors, interfaces, and others. The attack also impacted maritime systems including autopilots, radars, chart plotters, Automatic Identification Systems (AIS) sensors, sonar black boxes among others. GPS systems must be protected end-to-end by GPS providers and by those who consume GPS products and services.

IIoT

The Industrial Internet of things (IIoT) uses smart actuators and sensors to improve industrial processes. Transportation is growing IIoT faster than most other industries due to safety concerns. IIoT sensors create and track data such as train speeds, roadway temperatures, aircraft part conditions, and other critical information.[8] However, these devices are located outside centralized cyber-security perimeters making them vulnerable to several types of cyber attacks that can proliferate and cause damage throughout transportation environments.

Business and supply chain software

Transportation providers are tightly woven into today's integrated supply chains. As such, third-party software used for supply-chain integration and electronic payment systems used with 3rd-party partners is commonly used in transportation. These business applications are major source of vulnerability to transportation providers. The attack that cost Copenhagen-based A.P. Moller-Maersk A/S $300 million in 2017[9] came through financial software used by partners.

---

[8] Industrial-internet-of-things-iiot-market, GMI Research, August, 2020. https://www.gmiresearch.com/report/industrial-internet-of-things-iiot-market/

[9] Brendan Murray, Cyber Pirates Hit Global Shipping Industry Nearing Peak Season, Bloomberg, October 2, 2020. https://www.bloomberg.com/news/articles/2020-10-01/global-shipping-industry-hit-with-second-cyber-attack-in-a-week

How transportation providers can prevent threats

The problem with security controls in transportation is the large number of vectors that bad actors can attack. In addition to those mentioned above, mobile devices like smart phones, cloud-based applications, and software as a service (SaaS) must be protected. The usual method of deploying point solutions to protect each type of system creates a bewildering complexity for security staff members to monitor and manage. A survey revealed that thirty-five percent of the transportation-security professionals interviewed admitted they saw thousands of security alerts each day, but only investigated 44 percent. Of these, they remediated only 33 percent.[10] The answer to complexity is two-fold: preventative security and consolidated security architecture.

Prevention

Preventative security stops threats outside of a transportation provider's computing environment before damage is done and alerts are generated. Today, advanced threat prevention can use several methods. AI-based threat prevention learns to recognize and stop new, unknown threats by using input from massive numbers of sensors in the wild. Another method of advanced threat prevention blocks threats at the chip-level. Preventative security is most effective when integrated into a consolidated security architecture that covers a transportation provider's entire threat surface.

Consolidated Security Architecture

One reason for consolidated security architecture is that all security engines should be able to share threat information to avoid security gaps inherent in using a patchwork of standalone point solutions. Sharing threat information is important because of today's multi-vector threats. As important as threat sharing, consolidated security architecture also gives limited cyber security staff members a panoramic view of all security controls in all computing environments through one interface. Experts estimate that today it takes 60 or more security engines to provide complete coverage of all cyber threats. Consolidated architecture streamlines security monitoring, administration and management to reduce the burden on the cyber security staff.

[10]Melony Rocque, The cyber security threat to transportation, Smartcities world, as viewed on December 23, 2020. https:/www.smartcitiesworld.net/special-reports/special-reports/the-cyber-security-threat-to-transportation

Conclusion

The COVID pandemic is accelerating transportation's digital transformation. Migrating to preventative security deployed in a consolidated security architecture will put transportation providers on the right track to effective cyber security.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com