ProTecht
Solutions Partners, LLC
You have the Need, We provide the Solution

Securing the Intersection: A Look at Physical ITS Vulnerabilities

A White Paper for the ITS Community

Jon Polly

August 1, 2020

Introduction

Everyone who owns a car, no matter what country they are in, depends on traffic intersections. Whether they stop at the light, or they drive through the intersection at break neck speeds, those intersections are there for the safety of drivers and to enhance traffic flow to create a balance between protection and favorable customer experience. Many intersections today are security vulnerabilities waiting to adversely affect drivers and cities.

Vulnerabilities are just that … until a threat actor arrives and exploits them to do damage to the physical and cyber infrastructures of the Intelligent Transportation Systems (ITS). ITS technologies improve transportation safety and mobility, reduce environmental impacts, and enhance productivity by integrating advanced communications-based information and electronic technologies into the transportation infrastructure and vehicles. The momentum of technology development for connected vehicles (CV) and soon fully autonomous vehicles (AV) for the masses is bringing intelligence to a stage of innovation we have not seen in the past. (Although this paper uses information from the U.S. Department of Transportation, the solutions mentioned here have global application.)

Traffic Controllers

For many, intersections incorporate a traffic controller mounted in a box on the side of the road that must do several basic things. It must control the lights to keep people safe and keep traffic flowing. It should at its core transmit supervisory control and data acquisition (SCADA) data back to allow accurate notification of alarm conditions, and provide remote interaction with the controller for manual and automated timing adjustments, troubleshooting, and control actions. Most traffic controllers do many more functions than this.

In the aforementioned basic scenario, we see that the intersection is connected to at least two different city stakeholders. The City Department of Transportation (CDOT) controls the intersection. Information Technology (IT) controls the connectivity. Maybe these functions are in the same department, but for many cities, this involves two separate departments, each with its own set of controls and practices, and an agreement to work together.

Often, the practices and controls incorporated by each department do not sufficiently work well when it comes to large projects and ongoing infrastructure management; mainly due to each control method being siloed and managed separately without full collaboration. A simple example of this is the Traffic Control Box (TCB). The TCB incorporates a mixture of old and new technologies, with controls being shared between the CDOT and the IT departments, if not others. This mixture however brings physical vulnerabilities, technology vulnerabilities, and connectedness vulnerabilities; each of which can lead to a breach that breaks not just one system, but multiple systems. Furthermore, the design of the TCB has not received a significant upgrade in many years. Components have been changed and the physical relays have now migrated to electronic ones, but many of the same physical vulnerabilities that existed 50 years ago still exist today. With the addition of electronic and network attached devices, many of them not monitored or hardened for new cyber threats, the TCB now has physical hardware vulnerabilities plus remote connection vulnerabilities that did not exist in the past 50 years. Now that

cities today are being targeted like they have never been targeted in past, these vulnerabilities are more likely to be exploited. While the physical vulnerabilities may not have been exploited to date, cities cannot rely on history to protect them from threat actors.

Bombs and planes get the attention of the world, while cyber terrorists cripple corporations and cities with the press of a button while sipping a cup of coffee. The threat actor cares primarily about mayhem and money. On a citywide scale they can affect both greatly. This is one reason the U.S. Department of Transportation ITS Strategic Plan, 2016-2022 has outlined a Strategic Goal for the Development of Innovation; to encourage, coordinate, facilitate, and foster world-class research and development to enhance the safety, security, and performance of the Nation's transportation system. The current ITS system is exposed, putting drivers and cities at risk.

Implementing a strategy to effectively meet the goal will require that cities engage in a level of cross-silo collaboration between local stakeholder(s) and potentially State or Federal stakeholder(s), which most have not engaged in before. The strategic use of external resources can facilitate this level of collaboration, while creating a solution specific to the city's unique application and resources.

Current Challenge

Operational Technology (OT) and Information Technology (IT) have stayed relatively in separate silos, but that is changing. There is a convergence underway between OT such as traffic control systems, and IT to incorporate additional "Internet of Things" (IoT) sensors. Notwithstanding this convergence is the CDOT intersection. Many intersections already have multiple IoT sensors, be it surveillance cameras, signal timing cameras and equipment, additional vehicle and infrastructure communication. Today the TCB located at every intersection is an open gateway to the city. It is a mostly unsecured network enclosure with direct access to the city's core network, as well as the DOT core traffic platform.

In a day and time where cyberattacks are continuous and crippling to cities, the TCB offers mostly unrestricted access to the city's network. This unrestricted access will be exploited to cripple a city's ITS infrastructure and cause a loss of revenue either through ransom or loss of time and equipment. In 2019, more than 70 municipalities from large to small suffered ransomware attacks. That number looks to increase both in number and lost revenue. CDOTs can no longer assume "It won't happen to me", but rather to have the stance that "It will happen unless we do something". Securing the TCB is not the only way to stop cyberattacks, but it is how CDOTs can address vulnerabilities they control. Assume it will happen, and prepare for the best.

City IT departments have servers of all shapes and size. They have datacenters in multiple locations on a fiber ring for redundancy and security. They secure these devices behind firewalls, access control, and security protocols that are designed to keep the threat actor out. For CDOT intersections, the TCB houses many of these same technologies, with almost free access; almost. Most cities still are using a Corbin Cabinet Lock #2 key. This is the key that fits the lock developed in 1974 and is still installed on most TCB cabinets today. Today, this key can be purchased on auction sites like eBay for approximately $8 dollars. For $8 dollars, a threat actor can get into a majority of the TCBs installed in the United States. With a little research, they may find it is a CCL #3 key, or some specialized key. Nevertheless, physical entry to a TCB is very easy to attain. Many of the TCBs have a tamper or door status switch,

however these are rarely monitored and even if they are, they are rarely checked upon. For many, there is no reportable data for access granted.

It is time for an upgrade to the TCB that ensures the IT and the ITS infrastructure is protected, allowing drivers to be safe, traffic to stay flowing, and city networks to run with less vulnerabilities.

Scenarios

Minor Scenarios

What damage can the threat actor do? Let's start with the smallest issue. Shut down a single intersection during rush hour. This can cause a slight annoyance, but can be overcome. To take it a bit further, many of the TCBs are operated in either a daisy chain communication or a Hub and Spoke model. Find the Hub or find the first TCB in the line, the threat actor can take out multiple intersections. Maybe that's a bad day. Or maybe they do that on a day when the President schedules a visit and pandemonium ensues. These are all bad scenarios, but they are not the sinister scenarios.

Sinister Scenario #1

Most TCBs have network security at layer 2 or layer 3 of the Open Systems Interconnection Model (OSI model). This includes common security controls like port security, mac address filtering, VLANs, and routing. But once the Layer 2 or Layer 3 security is defeated, nothing is stopping the threat actor. That is where the sinister scenario happens. With the aforementioned $8 dollar key to gain access to the TCB, the threat actor with a cheap laptop, two pieces of free software and ransomware can begin an unmanned attack on a city, and they can duplicate this at each connected intersection. In this situation, the threat actor doesn't have to find the Hub or the first device in the daisy chain. A successful ransomware attack like this will cripple the city; delaying current and future city goals, notwithstanding the immediate issue that the entire ITS system may be infected creating citywide gridlock.

CDOTs have already been targeted through traditional means before today. But history shows, threat actors rarely stop. Many cities and businesses have experienced physical attacks that led to cyberattacks. The Broken Windows Theory by Kelling and Wilson still applies here. Once the first "break" is publicized, the city increases its chance of becoming a repeat victim of cyberattack.

Sinister Scenario #2

Connected Automated Vehicles are increasing every day. Many vehicles manufacturers today include dedicated short range communication (DSRC) radios in cars and trucks today for a variety of reasons, the impact is that the ITS community is seeing the need to deploy DSRC radios in each of its Traffic Control Boxes today. The DSRC radio's range is approximately 25-30 feet and creates a vehicular ad-hock network (VANET) between the TCB and the vehicle and provides real-time data about the intersection to the approaching car. The data includes pedestrian traffic, color of light, and emergency traffic, among other information. These VANETs are the basis for the vehicle to vehicle (V2V) communication that allows cars on the road to know what other cars on the road are doing. These are smart automobiles to say the least. But here is where the typical turns to the sinister.

DSRCs are wireless endpoints using a very specific FCC frequency range, 75 MHz of the 5.9 GHz Radio Spectrum; however the FCC has recently proposed pulling 45 MHz of this spectrum for new public WiFi, limiting how much spectrum DSRC radios will have to communicate. DSRC endpoints connect to most modern vehicles to provide or receive data. By using a TCB's internal DSRC radio, a threat actor could pass a virus to every connected vehicle that passes by. That virus could then be passed along the V2V connected devices. A simple virus could disrupt traffic; cause the connected or autonomous vehicle to behave erratically impeding safety, thus causing traffic congestion or accident(s). Each vehicle affected could then affect other vehicles. Another version of this attack could promote ransomware or other debilitating software that immobilizes the vehicle; causing both monetary losses to the owner as well as the aforementioned damages to the city infrastructure.

At the core, cyberattacks are being experienced daily at various levels of severity. Can a CDOT chance the risk of propagating such attacks? While vehicle owners must continually update vehicle firmware to prevent vehicle-side vulnerabilities, CDOTs must continually harden the TCB to prevent the scenarios above.

Steps to Securing the TCB

CDOTs cannot be blind to budgets. Many cities operate with limited budgets and every project must be vetted for value and urgency. Securing a single TCB is an inexpensive budget item. Securing all the TCBs in a city is significantly more costly. A layered approach of adding controls to create a protection in depth model must be implemented. This approach can be implemented in phases for cost effectiveness, but must be initiated with haste as cities can no longer afford to leave even a single unsecured opening.

Step One – Securing the TCB Network

As mentioned above, the IT department (either internal to CDOT or an external department) has probably already secured the network in the TCB with OSI layer 2 and layer 3 controls, but that is not enough. One layer 2 control is Port Security, where the network looks at a device media access control address (MAC address). This is the unique device for any electronic device made. When a device is added to the network, the IT department takes record of the MAC address, hard codes it to a port, and anything else plugged into that port flags an alert. The alert is configured to shut the port down on the network to prevent access to the network. Typically the port security gives the device 5 minutes to re-negotiate and identify itself before shutting down the port. This time is configurable, but no matter the time, an open door is an open door. How much damage can be done in five minutes? As mentioned before, with two pieces of free software, and IP Scanner and MAC address spoof tool, and knowing where to look, the port security is overpowered and entry is made. Or maybe it is just a USB drive plugged into a DSRC radio installed in the TCB to transmit a Distributed DOS (DDOS) or ransomware attack.

There are many ways to exploit an attack on the layer 1 or physical layer of the network bypassing all current IT controls. The physical security layer of the network is vulnerable and must be addressed with rogue device mitigation tools. The physical layer is where Internet of Things (IoT) sensors live. With Standards like NIST 800 this layer is has been introduced as the weak link. Most systems have network

monitors that show devices online or not, but there are few systems that identify the rogue device on the edge device and create alerts to shut the port down. Rogue Device Mitigation platforms identify a device by checking each device's known hardware profile, just like a digital fingerprint. If the fingerprint does not match, an alert is executed. This is tied to existing Layer 2 monitoring platforms; platforms that the IT resource have probably already deployed.

Physical layer security goes deeper than checking a spoofed MAC address or capturing a rogue USB drive. It negotiates the fingerprint of every attached peripheral edge devices. These devices may be cameras loaded with malware, USB devices with phishing software, a mouse loaded with a virus, or a Bluetooth skimmer. These are devices than can be deployed both by internal and external threat actors.

Today, the core IT datacenter is protected, maybe better than Fort Knox. The edge devices and edge networks are the vulnerabilities in any network. The ITS infrastructure is not without this vulnerability. By securing the physical layer of the network at the edge, the IT infrastructure is secure and a deeper alliance between CDOT and IT is initiated.

Step Two – Securing the TCB Cabinet

All TCBs should have a mechanical lock of some type in the event of power loss to the TCB, but keys are not enough to secure the TCB. Advances in electronic access control now make securing the TCB easier and cost effective, limiting the user's access and enabling reportable data for each site.

With any access product, be it a mechanical key, an electronic key, access card / fob, or a Bluetooth credential, a proper key management policy is paramount to security. While access cards and Bluetooth credentials are minimal cost, they must be managed to prevent unauthorized access. High security mechanical keys and electronic keys can be costly devices and should be tracked for security and asset management reasons.

Mechanical keys are what most CDOTs use today. At the very least mechanical locks should be changed from the 1974 Corbin Cabinet Lock to a more secure lock with high security keys. The keys should be keyed to a keyway specific to each CDOT. While many cities have State DOT roads and state owned TCBs, but are maintained by the local CDOT, it would need to be determined on a case by case basis as to which keyway was installed. There are multiple companies who have created a key only version that is a direct replacement for the 1974 CCL Lock, but then key management becomes even more critical. High security keys are both expensive to purchase and duplicate.

There are number of vendors who have created electronic access control locks specific to the TCB. These solutions can be purchased pre-installed by the TCB manufacturers or post install as a bolt-on upfit either by a vendor or by CDOT employees. Some solutions have recurring license costs and all solutions should be vetted prior to selection. In a properly designed system, with the advances of today, CDOTs should consider who would have the keys. Many CDOTs have given out the CCL#2 key to contractors and vendors to the point they cannot track the keys. For the contractor or vendor it is advisable to provide them either with physical access control credential or Bluetooth credential. This credential can be activated or deactivated as needed so unrestricted access is not gained. By providing an electronic credential to access the TCB, a log is kept of each access transaction and can be used to

show when access should have been made or not. Although many contractors, vendors, and staff are trustworthy, oversight is still required. True access control is maintained and a process to review contractors' access should be incorporated. Solutions should be designed for each specific CDOT and may include one or more of these technologies.

A concern with electronic access control is how to power the reader during a power outage as these can occur due to outages on the power grid, vehicle accidents, or faulty wiring inside the TCB. For the access control point it should be tied to a UPS that is typically installed in a TCB. Many of the access control platforms require POE+ (48VDC) power input, they also offer a battery backup connection. These batteries should be considered now or in the future to be converted to Lithium Iron Phosphate (LiFeP04) batteries. LiFeP04 batteries are more expensive, they offer both higher temperature ranges and significantly longer life than traditional Lead Acid batteries.

This application is requiring traditional DOT providers to merge with traditional security integrators to provide a solution that works well and can be maintained. Many CDOTs maintain their own equipment and their engineering team will require training on installation and troubleshooting of this application.

Step Three – Continued Network Security and Refresh Plan

Electronic manufacturers release security updates frequently. Firmware updates are necessary and are rarely completed. Updating is time consuming and if done improperly can have devastating effects. Not completed and it risks security vulnerabilities. Continued diligence to update the firmware and appliances are critical to the ITS network. This can be difficult if not impossible due to the age of the equipment and the staff involved. Failure to do these however will result in a vulnerability that can be exploited. When initiating controls, a holistic approach must be taken as the controls are interwoven. If one control is initiated, but not all, the vulnerability is still there.

Today many IT standards require unique passwords to be created every 90 days and are religiously changed to keep with the current standard. However the appliance the password is being connected to may be three or four firmware revisions behind; either because there is no time to update, or because the update will break other connected systems.

The latter scenario must be addressed. Manufacturers of electronics will provide information stating the mean time between failures (MTBF) of devices. This information is documented; can a CDOT wait until an appliance (switch, controller, etc.) fails? Today, that is what many CDOTs do. They purchase additional equipment and store it until something fails, or in many cases damaged by a vehicle accident. CDOTs cannot rely on the MTBF number. As important as updating firmware and passwords, CDOTs must plan for a refresh of equipment every 5 years. Most manufacturers offer no more than a five year warranty, if that. Many manufacturers either end of life (EOL) equipment or just stop updating firmware in preference to the newest model. The amount of technology changes that occur in five years makes equipment that is still functioning outdated and vulnerable.

Depending on policy and preference, CDOTs may choose to upgrade firmware and passwords internally. This may also become a function of the IT department but should have a report kept on hand of when the last updates were performed.

Outcomes

The immediate outcome with securing these edge devices is a safe and reliable network protecting the SCADA data, reducing traffic accidents, and keeping traffic flowing; providing a better customer experience and attracting new residents and visitors to the city over time.

CDOT is on its way to meet the US Department of Transportation ITS Strategic Goal for the Development of Innovation.

Cybersecurity of the VANET and V2V networks is achieved. The edge is secured and vehicles keep moving safely.

CDOT personnel receive new training on security installations and maintenance. CDOT creates policies and procedures on updates to be performed and how they are performed with metrics to be reported.

Key management solutions are implemented, forgoing retrieval of all missing or misplaced keys resulting in better asset control techniques and communication between CDOT and its Contractors and Vendors.

Reports are generated from multiple sources providing accurate logs of access, software and firmware updates, password controls reporting, as well as many custom defined reports.

The city has a successful inter-departmental collaboration that can be referenced and duplicated in other departments across the city.

Jon Polly is the Chief Solutions Officer for ProTecht Solutions Partners (www.protechtsolutionspartners.com), a security consulting and project management company, and has worked as a Project Manager and System Designer for City-Wide surveillance and Transportation camera projects in Raleigh and Charlotte, N.C.; Charleston, S.C.; and Washington, D.C. He is certified in Critical Chain Project Management (IC3PM) by the International Supply Chain Education Alliance (ISCEA).

Ray Bernard, of RBCS (www.go-rbcs.com) contributed to the review of this paper.

Sources

Cerrudo, Cesar. "Council Post: Cities Are Facing A Deluge Of Cyberattacks, And The Worst Is Yet To Come." *Forbes*, 18 Apr. 2018, www.forbes.com/sites/forbestechcouncil/2018/04/18/cities-are-facing-a-deluge-of-cyberattacks-and-the-worst-is-yet-to-come/#649630322559. Accessed 13 June 2020.

Dawson, Doug. "FCC Proposes New WiFi Spectrum." *POTs and PANs*, 23 Dec. 2019, potsandpansbyccg.com/2019/12/23/fcc-proposes-new-wifi-spectrum-2/. Accessed 26 July 2020.

Dopart, Kevin, and Kate Hartman. "USDOT's Vision for a Smart City THE SMART CITY CHALLENGE" Factsheet.

Federal Communications Commission. "FCC Seeks to Promote Innovation in the 5.9 GHz Band." *Federal Communications Commission*, 17 Dec. 2019, www.fcc.gov/document/fcc-seeks-promote-innovation-59-ghz-band-0. Accessed 26 July 2020.

Havelt, Rob, and Bruno Oliviera. *Hacking the Fast Lane: Security Issues with 802.11p, DSRC, and WAVE A White Paper for Black Hat DC 2011*. 2011.

Howard, Bill. "V2V: What Are Vehicle-to-Vehicle Communications and How Do They Work? - ExtremeTech." *ExtremeTech*, 6 Feb. 2014, www.extremetech.com/extreme/176093-v2v-what-are-vehicle-to-vehicle-communications-and-how-does-it-work. Accessed 13 June 2020.

Intelligent Transportation Systems Joint Program Office. "Intelligent Transportation Systems - How Connected Vehicles Work." *Www.Its.Dot.Gov*, www.its.dot.gov/factsheets/connected_vehicles_work.htm. Accessed 13 June 2020.

ITS Professional Capacity Building Program. "Academic White Paper - University Programs in Intelligent Transportation Systems (ITS): The Evolving Transportation Engineering Discipline - ITS Professional Capacity Building Program." *Www.Pcb.Its.Dot.Gov*, Nov. 2015, www.pcb.its.dot.gov/documents/whitepaper_university_pgms_in_ITS.aspx. Accessed 13 June 2020.

Jean.yoder.ctr@dot.gov. "National Highway Traffic Safety Administration." *Nhtsa.Gov*, 26 Oct. 2016, www.nhtsa.gov/technology-innovation/vehicle-cybersecurity. Accessed 13 June 2020.

Joint Task Force. "Security and Privacy Controls for Information Systems and Organizations." *Nist.Gov*, 2017, csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft. Accessed 13 June 2020.

Kelling, George L, and James Q Wilson. "Broken Windows." *The Atlantic*, The Atlantic, Mar. 1982, www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/. Accessed 8 July 2020.

Leonard, Ken. “DEDICATED SHORT-RANGE COMMUNICATIONS (DSRC) AND SPECTRUM POLICY.”

MacMichael, Duncan. “Windows Network Architecture and the OSI Model - Windows Drivers.” *Microsoft.Com*, 20 Apr. 2017, docs.microsoft.com/en-us/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model. Accessed 15 June 2020.

Rawat, Ajay, et al. “VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS.” *Journal of Information and Operations Management*, vol. Volume 3, no. Issue 1, 15 Jan. 2012, pp. 301–304, www.academia.edu/3203478/VANET_SECURITY_ATTACKS_AND_ITS_POSSIBLE_SOLUTIONS, 10.9735/0976-7754. Accessed 13 June 2020.

Sarah.henderson@nist.gov. “Before Connecting an IoT Device, Check Out a New NIST Report for Cybersecurity Advice.” *NIST*, 27 June 2019, www.nist.gov/news-events/news/2019/06/connecting-iot-device-check-out-new-nist-report-cybersecurity-advice. Accessed 13 June 2020.

Schneier, Bruce. “Class Breaks | Edge.Org.” *Www.Edge.Org*, 30 Dec. 2016, www.edge.org/annual-question/2017/response/27229. Accessed 8 July 2020.

US Department of Transportation. “DOT Strategic Plan for FY2018-2022 | US Department of Transportation.” *Www.Transportation.Gov*, 13 Feb. 2018, www.transportation.gov/administrations/office-policy/dot-strategic-plan-fy2018-2022. Accessed 13 June 2020.

US Department of Transportation. “Intelligent Transportation Systems - ITS Strategic Plan 2015-2019.” *Www.Its.Dot.Gov*, Dec. 2014, www.its.dot.gov/factsheets/itsjpo_stratplan.htm. Accessed 13 June 2020.

Voas, Jeffrey. “Networks of ‘Things.’” *Csrc.Nist.Gov*, 28 July 2016, csrc.nist.gov/publications/detail/sp/800-183/final. Accessed 13 June 2020.

Wikipedia Contributors. “Dedicated Short-Range Communications.” *Wikipedia*, 8 Jan. 2020, en.wikipedia.org/wiki/Dedicated_short-range_communications. Accessed 13 June 2020.

Wikipedia Contributors. “OSI Model.” *Wikipedia*, Wikimedia Foundation, 11 Mar. 2019, en.wikipedia.org/wiki/OSI_model. Accessed 13 June 2020.

Wikipedia Contributors. “SCADA.” *Wikipedia*, Wikimedia Foundation, 24 Oct. 2019, en.wikipedia.org/wiki/SCADA. Accessed 13 June 2020.