| feature

shutterstock.com/ Maksim Kabakou

Cyber Security Challenges:

Protecting Your Transportation Management Center

By Edward Fok, P.E., PTOE

A Transportation Management Center (TMC) is the heart of many critical transportation systems. In order to make TMCs more resilient to cyber-attack incidents, operators should have an understanding of the nature of the threats, their own vulnerabilities, and their capability to respond. This article walks through the fundamentals of common cyber-attack processes and offers ideas on how to prepare and respond to an incident.

What would happen if the United States could not:

1. Safely operate the transportation infrastructure for all modes?
2. Efficiently operate the systems to facilitate movement of people, goods, and services?
3. Communicate with the public for the public's interest and safety?

The TMC is frequently the nexus where these common objectives of the transportation systems are carried out day to day. Preservation of these capabilities is why protecting the TMC from a cyber-attack incident is so critical.

As part of Executive Order 13636, Improving Critical Infrastructure Cybersecurity, the U.S. Department of Transportation (USDOT) developed a Cyber Security Action Team charged with the implementation of the Department's Cyber Incident Response Capability Program. This team will leverage the extensive body of assessments and research done by Federal Highway Administration (FHWA) staff related to the security threats and vulnerabilities of the United States' transportation systems. This insight, an important aspect of the Department's overarching "transportation operations domain expertise," is offered through a series of articles that began in the July 2013 *ITE Journal* with the article, "An Introduction to Cybersecurity Issues in Modern Transportation Systems."[1] This article series serves as an introduction to strategies for organizations to meet new challenges to the modern transportation system and are not meant for training. While the first article gave an overview of the cyber risks to the overall transportation system, this article will focus on the security of the TMC.

TMCs will have a number of common components as shown in Figure 1, and although there are numerous possible configurations, this will provide the generic framework for this article.

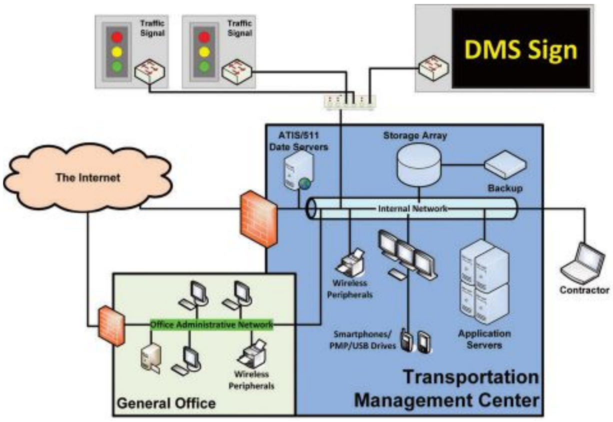


Figure 1. Common network layout of a transportation management center.

Courtesy of the Federal Highway Administration

Who are the attackers?

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has broadly defined three groups of "Threat Agents."[2] Group 1 could include almost anyone with the requisite technical knowledge. The reprogramming of portable dynamic message signs (DMS) signs for "fun and notoriety" among peers is an example of a Group 1 threat. Group 2 includes organized crime syndicates, activist groups, insiders, disgruntled employees, and hacktivist groups such as "Anonymous." Ransomware viruses are examples of Group 2 threats. Group 3 includes terrorists and nation states engaged in cyber warfare. While most attackers use a similar process in their assaults, what distinguishes one threat agent group from another are the degree of motivation and the extent of available resources. A Group 3 attacker will have significantly more resources available than a Group 1 attacker.

Step 1: Breaching the Network

A breach occurs when the attacker is able to get on the protected TMC network. A breach could be analogous to an uninvited person walking into your home. The act itself does not automatically translate into a threat to life and property. It could be very disturbing and sometimes the intruder could spray paint the wall or commit some other random acts of vandalism, but no real lasting harm may result by the breach. A cyber security breach could have a physical component, especially when someone breaches an "air gapped" TMC network. The point where an attacker can breach your network is called an "attack surface." A network with many possible entry points is said to have a large attack surface. Common attack surfaces into a TMC network could include:

1. Poorly configured field network devices;
2. Malware delivered using email or a compromised website;
3. Malware walked in by a user either inadvertently or deliberately;
4. Compromised partner networks;
5. Poorly configured external firewall, switches, or agency webpages;
6. Compromised user credentials; and
7. Unauthorized physical entry.

Step 2: Scanning and Mapping

Once the attacker has breached the network, they have to find out what is in it in order to attack deeper. Using the same analogy, the intruder is now going through your home trying to understand its layout and figuring out where the valuables are hidden. They could install automated monitoring software (spyware) to learn the behavior of the users and identify other devices on the network. Important information such as unencrypted passwords between a client and server, username, and user identity could be captured. This information is valuable for "exploitation." External Group 2 and Group 3 threat agents need to go through this step to target critical components. The attacker could take their time by inserting a "back door" to circumvent security and come back later to continue where they left off.

If the TMC is connected to other agencies and organizations (such as contractors), scanning and mapping could expose these additional organizations to the intruder. If the trust verification mechanism between partners is weak, this could allow an attacker another way to bypass the security of a protected system.

Step 3: Exploitation and Egress

Exploitation is when the intruder becomes an attacker. The information collected in Steps 1 and 2 becomes a roadmap for the attacker to accomplish his/her goals. USDOT is fortunate not to have had any confirmed reports of a successful TMC attack, but has seen what can happen when TMC systems crash, and what happens when transportation systems are targeted by hacktivists.[3,4] There are cases where victims have been threatened with a massive release of personally identifiable information (PII) or other critical files unless a ransom was paid, or just denial of access to critical files in exchange for ransom.[5,6,7] These incidents have shown the importance for having a backup plan.[8]

It is important to keep in mind there is a difference in perceived "value" of resources between a TMC operator and an attacker. What is important to an operator could be worthless to an attacker while operational support systems could be very attractive. For example, an arterial TMC could place a high value on their closed caption television (CCTV) and signal control system. An attacker probably will not have the skill needed to exploit the CCTV and signal control system, but they could cripple operations by deleting critical files needed by the TMC servers.

We also assume that an attacker is unable to interpret the data message used by our control systems.[9] However, the attacker can target the workstation where the information is presented to the operator. In this type of attack, there is no need to understand National Transportation Communications for ITS Protocol (NTCIP) or Traffic Management Data Dictionary (TMDD) data objects. The attacker remotely controls the workstation and may press the on-screen button that says "Flash Red." It is frequently dangerous to underestimate the determination of a Group 3 attacker to understand and exploit vulnerabilities in the target.

Egress could be an important element in a successful attack. If an attacker wishes to remotely control the operator's workstation, they must establish a data connection out of the TMC. Unless they opened up a new data connection using a rogue device, they are probably using the same network route they used to come in.[10] It is important to note that successful attacks may not require an egress.[11]

Special Topic: Denial of Service Attack

A Denial of Service (DOS) attack attempts to overwhelm a network by flooding it with massive amounts of communication, typically against internet facing application and components. DOS attacks can take place without the typical breach, scan, exploit, egress attack cycle. This type of attack is similar to someone ringing your doorbell and running away–repeatedly. They keep interrupting you (analogues to the server) from doing your work since you (as the server) have to respond to every ring of the bell. To magnify this, the attacker could ask his friends to do the same thing, or to knock on the windows and the backdoor at the same time. In some cases, they could put a sign up at the nearest major road asking passersby to press your door bell for a chance to win a prize!

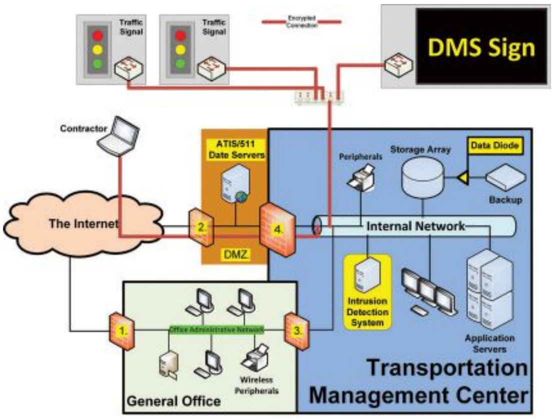
DOS attacks are very difficult to defend against, and they are relatively inexpensive to launch. A 2011 sample showed 32 percent of attacks were under 10Mbps in size, and 76 percent were less than 1Gbps.[12] To put these values into context, each of the cyber riots that crippled communication throughout the country of Estonia averaged between 100Mbps to 200Mbps,[13] peaking occasionally up to 40Gbps.[14] Modern DOS attacks could generate enough traffic to slow down the entire Internet.[15] Using information from a successful scan of a targeted network, a sophisticated and targeted attack could be successful using a lower volume of traffic.

We Can't Stop Them All, But We Can Make It Harder

We can make cyber-attacks harder by interrupting as many of the attacker's steps as possible. The methods described here are based on hard lessons already learned by the information technology (IT) and e-commerce industries. Losses in those industries frequently result in immediate and extensive economic losses and carry legal repercussions.[16] The overarching theme is "Defense in Depth," as there is no magic shield to defend the TMC. All networks can be breached and exploited to some extent given enough time and resources.

Stopping Breaches

Many of the mitigation methods mentioned in the previous article will be useful to limit the attack surface of a network. It is important to include the TMC staff and staff from other departments as potential attack surfaces using "social engineering" methods. Some of these risks can be assessed using the Cyber Security Evaluation Tool (CSET).[17] Techniques such as network segmentation, proper deployment of firewall (items 1–4 in Figure 2), and best practices in edge device configuration are well known to the information technology community.[18] Each agency should have an IT and information security policy that is understood and followed by TMC operators. TMC staff and management should be trained to identify and defend against social engineering attempts.



COURTESY OF THE FEDERAL HIGHWAY ADMINISTRATION

Figure 2. A possible network configuration for a more secure TMC.

TMCs are frequently open to visitors and public tours. These visits are an opportunity for potential attackers to create a new attack surface or even breach an air-gapped network. Each agency also should have a visitor policy that is commensurate with the perceived risk of their transportation system. A high risk TMC could take additional steps such as eliminating physical features where rogue devices can be hidden or consider designating a visitor-only area. Attackers motivated enough to breach an air gap network are probably Group 2 or Group 3 threat agents.

Disrupting Scans and Network Mapping

If an attacker can breach the network, they could be detected by watching for unusual activities on the network. An Intrusion Detection System (IDS) on the TMC internal network can help detect abnormal behaviors from field devices and other network components.[19] Also, a honeypot could be used to help trap intruders on the TMC's internal network.[20] Information collected about an attack could be useful to support future prosecution against the attackers.

Another technique is encrypting communication on the control network to make it more difficult for the attacker to understand the control system. There could be legal repercussions if an attacker illegally breaks encryption used on government systems. TMC operators should consult with their agency's legal department or Chief Information Security Officer (CISO) about this for their jurisdictions. Anyone attempting to break an encrypted network is likely well-motivated and could be a Group 2 or Group 3 threat agent.

Limiting the Effects of Exploitation and Locking the Gate

While an attack is underway, the most important task is to realize it is happening. Part of this requires vigilance on the part of the TMC operator and the IT support team. Executing an existing, well-understood response plan can help contain the impact. Most agencies are not prepared for a well-orchestrated cybercriminal, hacktivist, or cyber warfare attack from Group 3 and some Group 2 threat agents.

Most TMC data traffic between trusted partners is not monitored. This needs to change so operational partners do not become the source of attacks through an unprotected backdoor into the TMC network. For example: Does the support contractor really need a dedicated and unprotected data connection into your TMC internal network? Can the TMC operate without a normally connected partner?

Restoring the TMC systems from backup is a fast way to resume operation in case of a catastrophic loss. Frequent backup of all critical application and databases is crucial and the backups must be protected. For systems such as traffic signal control, the parameters on the local controller should be kept current to allow local control to take over if TMC is compromised.

Defending Against DOS Attacks

A number of techniques exist to slow down or delay modern DOS attacks. The best defense is to stop an attack at the Internet Service Provider (ISP). DOS attacks typically come from the Internet, and mitigation measure is most effective at the connection to the Internet. Because most DOS attacks will target the ATIS/511 server, a solution could include moving the server into the Demilitarized Zone (DMZ)[21] of the network, keeping it separated from the internal network with a backend firewall (item 4 in Figure 2). This will allow an attack to wipeout this server without affecting your core function.

Moving forward

Now that we have some basic idea on how an attack could take place, here are some steps that should be considered as part of failure and resiliency planning for a TMC.

1. Know Your Vulnerability

One way to start could be the use of the CSET tool to better understand the vulnerabilities already present in the TMC. Vulnerability assessment should be a continuous process of evaluation and monitoring of the configuration and health of the TMC's IT infrastructure. If possible, review vulnerabilities during the planning phase of a new TMC.

2. Understand Your Risk

A TMC supporting transportation operations in a small rural community is probably at a low risk for a cyber-warfare strike. But the Center is likely to see Group 1 threat agents hacking the portable DMS signs. However, if this jurisdiction encompasses a national security facility, the TMC operators may want to reach out to the national security facility to see if the TMC's risk exposures are elevated. Along with risk assessment, TMC owners should determine the damage potential from a breach. If a rural or suburban TMC that monitors conditions via CCTV and performs basic health monitoring of field device was disabled, the immediate disruption could be limited. But disabling a TMC that utilizes cloud-based computing for real-time multimodal coordination in a highly congested region could result in a rapid and severe disruption to regional operation.

3. Know Your Limits

Be realistic in what can be supported by the TMC team, the IT support team, and the ISP by understanding the technical, legal, and institutional limits under which the team is operating. Use this information to develop a risk matrix and determine what risks are manageable by local staff, and which ones are not. Very few TMCs can respond to the full spectrum of cyber threats, so it is very important to know when the limit is reached and where to get help. In all cases, it is vitally important to continuously monitor activities and changes to the IT infrastructure. The ability to react starts with the awareness of the problem. Risk factors with high damage potential that cannot be managed by local staff should be aggressively monitored so problems can be detected as quickly as possible.

4. Have a Plan

Many TMCs already have plans that address operational issues such as roadway incident management, equipment failures, and natural events. Protecting the TMC's IT infrastructure deserves the same treatment and will take time and help from the IT support group. Fortunately, the IT industry has developed a number of resources that focus on the IT aspect of the problem. The *Roadmap to Secure Control Systems in the Transportation Sector* was created to help agencies develop such a plan and the culture needed to sustain it.[22]

The plan should include a procedure to manage reports of vulnerabilities discovered by "white hat hackers." Consider working with your agency's CISO to create a policy to properly respond if this were to happen.[23] The plan should take into consideration the three actions that can occur when vulnerability is discovered by a hacker:

1. The hackers could report the vulnerability to you. When you fix it, they will claim credit for discovering the flaw.

2. The hackers could widely disclose it immediately. Everyone will know about the flaw and if the vulnerability is severe, you have to race against time to close the vulnerability and prepare a public relations response.
3. They could sell it to a Group 2 or Group 3 threat agent who could use it against you.[24]

Once the plan is developed, make sure the TMC and IT team know how to execute it.

Conclusion

The difficulties facing TMC owners and operators can be alleviated by a closer relationship with their IT support resources. TMCs will have to accept that internal IT systems, in addition to the transportation infrastructure, need to be actively monitored. The security challenge will continue to increase as transportation infrastructure becomes more connected with greater levels of automation. While many of the mitigation approaches can be retrofitted to existing facilities, they are best applied during the initial stages of planning a new facility. **itej**

Additional Resources

Industrial Control System Cyber Emergency Response Team – Recommended Practices (http://ics-cert.us-cert.gov/Recommended-Practices)

References

1. Fok, Edward, "An Introduction to Cybersecurity Issues in Modern Transportation Systems." July 2013 *ITE Journal*. Washington, DC, USA: ITE.
2. "Strategy for Securing Control Systems." U.S. Department of Homeland Security. Washington, DC, USA: U.S. Department of Homeland Security, October 2009.
3. Ashley Halsey, "Traffic Signals Disrupted, Creating Chaos in Montgomery," *Washington Post*, November 5, 2009.
4. Fahmida Rashid, "Anonymous Hack Exposes Personal Data of San Francisco-Area Commuters," *eWeek*, August 8, 2011.
5. Brian Kerbs, "Hackers Break Into Virginia Health Professions Database, Demand Ransom," *Washington Post*, May 4, 2009.
6. Amanda Grace, "Swansea Police Dept. Targeted by PC Hackers," WHDH.com News, November 20, 2013.
7. "CryptoLocker Ransomware Infections," US-CERT Alert (TA13-309A), last modified November 18, 2013, www.us-cert.gov/ncas/alerts/TA13-309A.
8. Maryanne Twentyman, "Computer Virus Hits Ambulances," *Waikato Times*, November 12, 2011.
9. Jesper Johansson and Roger Grimes, "The Great Debate: Security by Obscurity," *Microsoft TechNet Magazine*, June 2008.
10. Sean Gallagher, "Pwned again: An Exclusive Look at Pwnie Express' Newest Hack-in-a-Box," *Ars Technica*, July 30, 2013.
11. Aviv Raff, "Shamoo, a Two-Stage Targeted Attack," Seculert.com, last modified August 16, 2012, www.seculert.com/blog/2012/08/shamoon-two-stage-targeted-attack.html.
12. N.J. MahWah, "Radware 2011 Global Application and Network Security Report," Radware.com, last modified January 27, 2014, www.radware.com/newsevents/pressreleases/global-application-network-security-report.
13. Robert Vamosi, "Newsmaker: Cyberattack in Estonia – What it Really Means," CNET News, May 29, 2007.
14. Charles Clover, "Kremlin Backed Group Behind Estonia Cyber Blitz," *Financial Times*, May 5, 2009.
15. Peter Bright, "Spamhaus DDoS Grows to Internet-threatening Size," *Ars Technica*, March 27, 2013.
16. Mark Huffman, "TJX Pays $9.75 Million To Settle Data Breach," ConsumerAffairs.com, last modified July 27, 2009, www.consumeraffairs.com/tj-maxx-data-breach.
17. The Cyber Security Evaluation Tool is available from www.us-cert.gov/control_systems/csetdownload.html.
18. ISO/IEC 27000, NIST Computer Security Resource Center, and "Standard of Good Practice" by Information Security Forum (www.securityforum.org) are all examples of guides that are used throughout the commercial sector to security computer systems and websites.
19. Karen Scarfone and Peter Mell, National Institute of Standards and Technology Special Publication 800-94: *Guide to Intrusion Detection and Prevention Systems*. Washington, DC: U.S. Department of Commerce, 2007, page 6-1.
20. Loras Even, "Intrusion Detection FAQ: What is a Honeypot?," Sans Institute, last modified July 12, 2000, www.sans.org/security-resources/idfaq/honeypot3.php.
21. Deb Shinder, "SolutionBase: Strengthen Network Defenses by Using a DMZ," *Tech Republic,* last modified June 29, 2005, www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz.
22. "Roadmap to Secure Control Systems in the Transportation Sector," prepared by The Roadmap to Secure Control Systems in the Transportation Sector Working Group, last modified August 2012, http://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/TransportationRoadmap20120831.pdf.
23. "How do we define Responsible Disclosure?," SANS Institute, last modified April 22, 2003, www.sans.org/reading-room/whitepapers/threats/define-responsible-disclosure-932.
24. Andy Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits," *Forbes*, March 23,2012.

Edward (Ed) Fok, P.E., PTOE *is a transportation technology specialist with the Federal Highway Administration (FHWA) Office of Technical Service/Resource Center. He helps public agencies apply advanced transportation systems and processes to solve mobility problems. He also helps researchers advance the state of the art in transportation operations. Ed came to FHWA from the City of Los Angeles, CA, USA with 11 years of experience. He holds multiple professional engineering licenses. Ed is a member of ITE.*