

Cyberattacks Against Intelligent Transportation Systems

Assessing Future Threats to ITS

Numaan Huq, Rainer Vosseler, and Morton Swimmer
Trend Micro Forward-Looking Threat Research (FTR) Team

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

for Raimund Genes (1963-2017)

Contents

5

The ITS Ecosystem

13

Real-World ITS Attacks

21

ITS Attackers

23

ITS Attacker Motives

27

ITS Attack Vectors

37

Threat Modeling the ITS Ecosystem

45


Securing the ITS Ecosystem

50

Conclusion

52

Appendix




In October 2014, the electric car manufacturer Tesla introduced their road-ready Autopilot system, a system that enables a car to autonomously detect obstacles, navigate roads, avoid pedestrians, and keep pace with traffic. This changed driving forever and created a bold new vision for how road networks will be used in the future. While it will take a decade or two for fully autonomous vehicles to become everyday roadway fixtures, the number of internet-connected cars on the road is already increasing. In the Industrial Internet of Things (IIoT) world, it is realistic to expect that someday, roadways will be upgraded to Smart Roads that are fully integrated with today's internet-connected cars and tomorrow's autonomous vehicles.

This future scenario of Smart Roads is but one aspect of the bigger picture of Intelligent Transportation Systems (ITS). Smart Roads and ITS are poised to play a crucial role in future urban planning and development, which aims to make high-volume traffic movement more efficient, improve road safety, create new economic opportunities, and reduce ecological and environmental impact—especially in countries with high urban population densities. This is why different government bodies (at the municipal, state, and federal levels) in Asia, the European Union (EU), and North and South Americas are actively investing in the development of ITS technologies and policies.

Aside from government agencies and policymakers, the IT security industry has also recognized the importance of ITS and its components. The IT security industry has been busy researching car hacking techniques, thereby discovering attack vectors against modern connected cars and trucks and future autonomous vehicles that enable perpetrators to seize control of vehicle functions, steal data, or both. Because the entire road-operating environment is critical to the safe operations of both modern and future vehicles, in this research paper, we looked beyond the attack vectors targeting connected cars and trucks and instead studied cyberthreats against the entire system. This entailed researching threats against Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I) communications as well as cyberthreats against ITS infrastructures such as automated toll collection, weather stations, traffic cameras, traffic signals, speed sensors, dynamic road barriers, navigation aids for autonomous cars, etc.

Until recently, attacks against ITS infrastructure have been few and far between. But as more connected vehicles drive on the road, these threats will increase over time, especially when criminals discover new profiteering models. ITS systems are highly visible and attacks against them will be high impact. Attacks against the ITS ecosystem can:

- 
- Cause vehicular accidents
 - Create traffic jams that affect essential services, freight movements, and daily commutes
 - Lead to a ripple effect that can cause financial loss to individuals, businesses, and municipalities

There is currently very little published research discussing the cybersecurity threats against ITS. In this paper, we first explored real-world ITS cyberattacks and their impact. As cyberattacks and attackers go hand-in-hand, we discussed the most likely perpetrators and their goals and motivations for attacking ITS. We then applied our knowledge of current cyberattacks to develop and analyze future cyberattack scenarios against ITS and Smart Roads. The ITS applications and systems (A&S) we studied were grouped into six categories: Vehicles, Roadway Reporting, Traffic Flow Control, Payment, Management, and Communications. Based on the probable worst-case impact to public safety and daily operations, we classified the ITS devices/systems into three Impact Severity Levels (ISLs):

- L1 — Applications and systems that directly affect public safety and critical operations
- L2 — Applications and systems that affect daily operations and revenue generation
- L3 — Applications and systems that support L1, L2, and the organization itself

We applied the industry standard DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability) threat model to assess cybersecurity risks against ITS devices/systems. Finally we provide a set of guidelines for protecting the ITS ecosystem against cyberattacks; these guidelines include technology discussions for IT security teams, and policy discussions for key decision-makers.

The ITS Ecosystem

Intelligent Transportation Systems, or ITS, is the application of advanced and emerging technologies in transportation to save lives, time, money and the environment.¹ This definition includes all modes of transportation, from ground and rail to marine and air travel. The scope of this research paper, however, only covers the threat of cyberattacks against connected cars, autonomous vehicles, and Smart Roads, as attacks on these will be more highly visible, have a more immediate effect, and potentially have a disastrous impact on public safety.



Figure 1. Intelligent Transportation Services

This section will examine the components of a typical ITS ecosystem: frameworks, vehicles, roadway reporting, traffic flow controls, payment applications and systems, management applications and systems, and communications applications and systems.

The ITS Framework

Highly complex systems such as integrated ITS applications require a strategic framework for design and deployment as well as identification of future investment areas. The ITS framework architecture is the blueprint that maps out all the technical aspects of ITS and allows designers and planners to visualize the organizational, legal, and business requirements. It also ensures that the resulting ITS deployment is logically planned, integrates well with other systems, and meets the performance and behavior requirements of its stakeholders and users. An ITS framework architecture helps make the entire ecosystem easy to manage, maintain, and extend. Compliance with a common ITS framework architecture will enable multiple applications to work in sync, even at multinational levels.² There are currently three major ITS frameworks being developed globally: the European ITS Framework Architecture, the U.S. National ITS Architecture, and the Japanese ITS System Architecture.

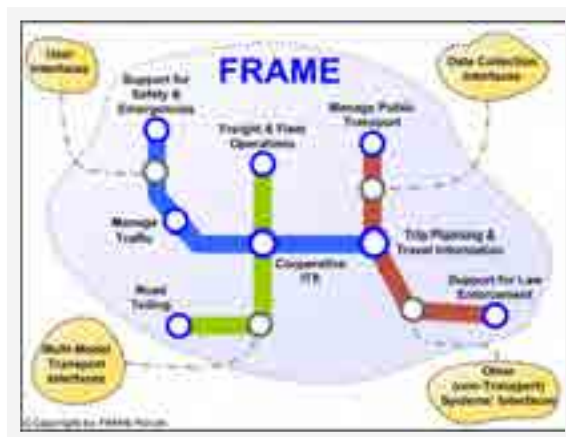


Figure 2. European ITS Framework Architecture, a.k.a. the FRAME Architecture
(Source: <http://frame-online.eu/>)

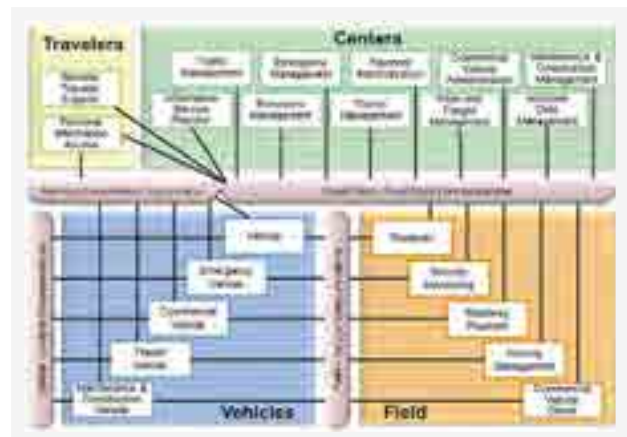


Figure 3. US National ITS Architecture

(Source: https://ops.fhwa.dot.gov/publications/telecomm_handbook/chapter3.htm)

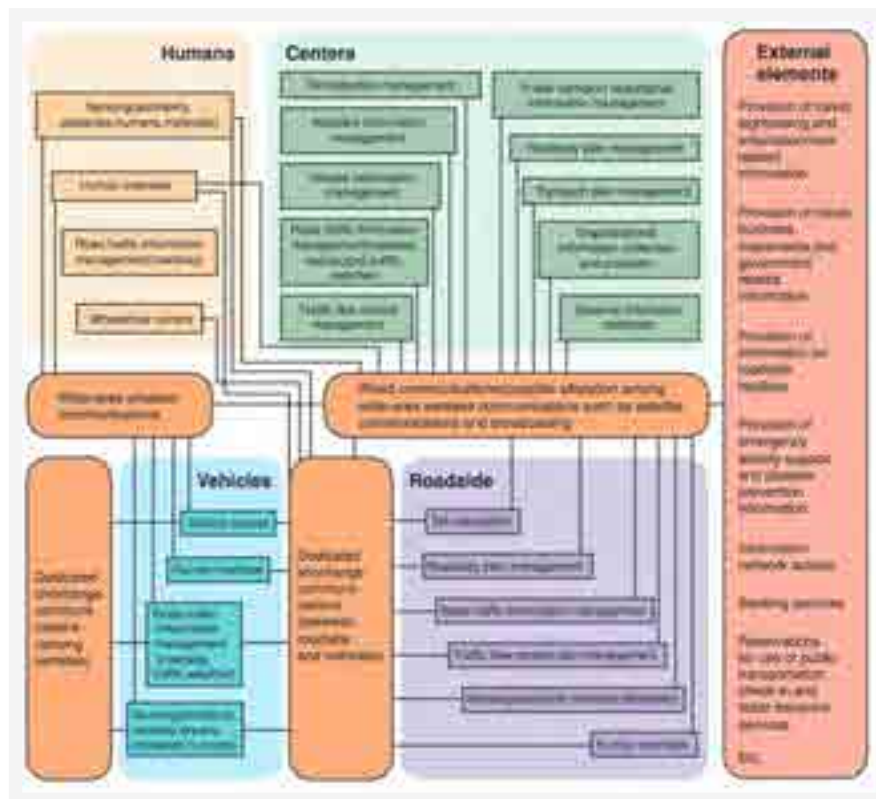


Figure 4. Subsystem Interconnect Diagram from the Japanese ITS System Architecture

(Source: <http://siteresources.worldbank.org/EXTROADSHIGHWAYS/Resources/ITSNote5.pdf>)

Based on these three ITS frameworks, we selected a subset of ITS applications and systems (A&S) that are most at risk of getting compromised by attackers. We grouped these ITS A&S into six main categories: **Vehicles, Roadway Reporting, Traffic Flow Control, Payment, Management, and Communications.** For an in-depth discussion of these ITS A&S, refer to the Appendix.

Vehicles

Vehicles (cars, trucks, buses, etc.) are fundamental components of transportation, and no ITS discussion is complete without talking about vehicles. This research focuses on two types of vehicles:

- Connected vehicle — Equipped with internet access and also has a wireless Local Area Network (LAN), which allows it to share internet access with other devices both inside and outside the vehicle.
- Autonomous vehicle — A more advanced version of the connected vehicle, one that is capable of sensing its environment and navigating without human input using a variety of technologies such as LIDAR, RADAR, GPS, stereoscopic cameras, etc.

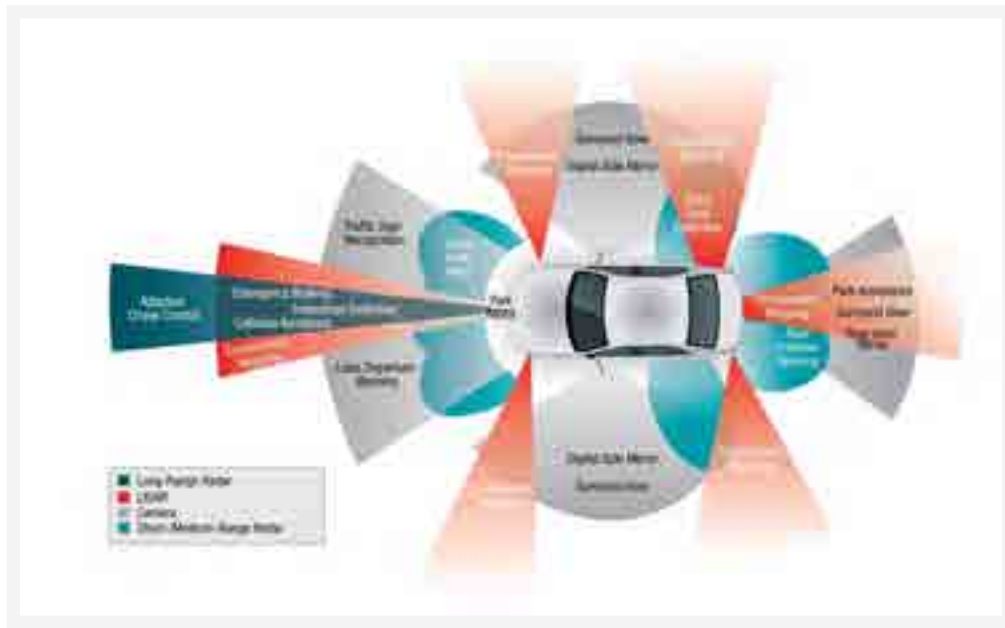


Figure 5. Car sensors and their effective ranges

(Source: http://www.sae.org/dlymagazineimages/15067_24935_ACT.jpg)

Roadway Reporting

ITS goals include making high-volume traffic movement more efficient and improving road safety. To achieve these goals, road operators need to constantly monitor traffic and current roadway conditions. This is done using an extensive array of cameras and sensors that are strategically placed all across the roadway and which sends back data real-time to the control center. Examples include: bus lane cameras, speed cameras, roadside weather stations, and vehicle detection systems.



Figure 6. Roadway monitoring & traffic flow control

(Source: <http://www.its-ukreview.org/smart-motorways/>)

Traffic Flow Controls

Similar to roadway reporting systems, traffic flow controls aid in making high-volume traffic more efficient as well as making roads safer. Road operators monitor traffic and roadway conditions in real-time and use gathered data to manage traffic flow using various flow-control mechanisms. Examples include: traffic signal control systems, railway crossing barriers, dynamic message signs, and automated toll collection systems.

Payment Applications and Systems

In addition to organizing traffic movement and making road safety better, one of the major goals of ITS operators is to use the systems in place to increase their revenue stream while reducing costs. Examples include: RFID payments/tags, kiosk payment machines, and e-ticket applications.



Figure 7. Toll collection in Singapore using Automatic Number Plate Recognition (ANPR)

(Source: <http://www.citiprop.com/living-in-singapore/>)

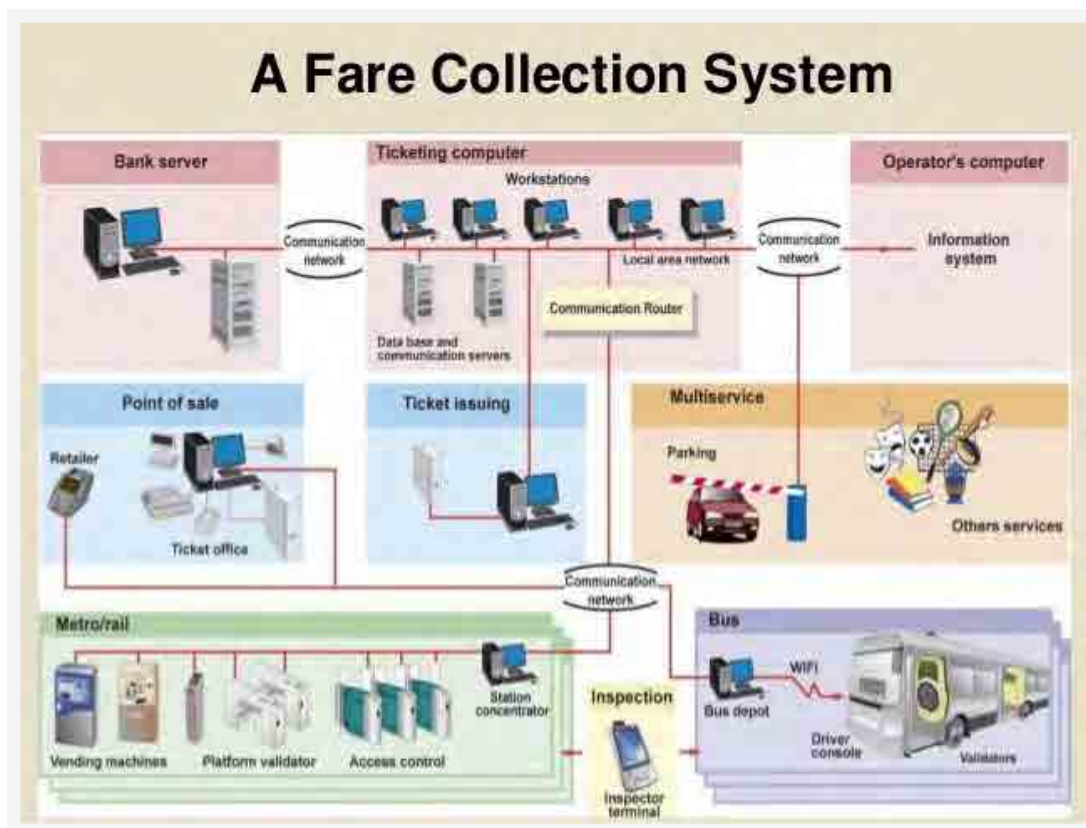


Figure 8. Multimodal fare collection system

(Source: <https://www.slideshare.net/NYPTA/implementing-contactless-fare-collection-systems>)

Management Applications and Systems

ITS is best described as a complex ecosystem comprising hundreds and thousands of connected systems with a wide range of functions, working cooperatively or in tandem. All systems need to operate within defined tolerance limits for traffic to flow smoothly; otherwise, there will be traffic jams, delays, accidents, and the like. ITS nerve centers host, monitor, and operate the management systems controlling ITS. Examples include: streetlight controls, disaster management, data and data storage management, emergency vehicle management, and traffic and congestion management.



Figure 9. Centralized controls for ITS management systems

(Source: <https://www.standards.its.dot.gov/ApplicationArea/5>)

Communications Applications and Systems

Information exchange is the core of the ITS ecosystem. Data is used for making traffic flow efficient, improving road safety, increasing revenue, and reducing ecological and environmental impact, among other uses. Data is also consumed by the users of ITS services to improve their transit options and experiences. Examples include: smart apps, social media, websites, and road obstacle and accident alerts.



Figure 10. Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I) communications in future roadways

(Source: http://media2.govtech.com/images/940*670/V2I+Communication+USDOT.jpg)

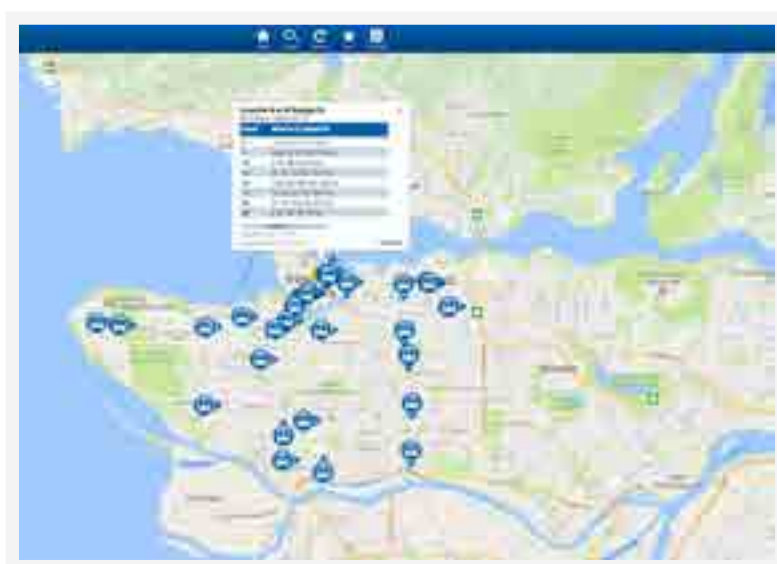


Figure 11. Vancouver's real-time transit bus location system

(Image generated from: <https://nb.translink.ca/>)

Real-World ITS Attacks

The interconnected ITS ecosystem that we described is not yet fully implemented. We are still at least a decade away from fully interconnecting every vehicle and every roadway ITS system. But even with the current ITS infrastructures in place, as more connected ITS systems are coming online, attacks are increasing. In this section we look at some of the real-world cyberattack incidents against ITS systems that have made recent news headlines.

- May 23, 2016. Dallas News reported a Texas man hacking and changing a highway sign to say “Drive Crazy Yall” as a prank. The culprit was identified as Geoffrey Eltgroth and was arrested and charged with criminal mischief.³ Eltgroth admitted to guessing the login credentials for the sign, deleting the original message to warn traffic of upcoming construction, and typing the prank message for humorous purposes.



Figure 12. The hacked traffic message sign

(Source: http://www.realclean.com/offbeat/2016/05/24/great_prank_leads_to_truly_terrible_advice_on_hacked_texas_road_sign_13439.html)

- June 6, 2016. The Washington Post reported that Dallas road signs were hacked and messages about Donald Trump, Bernie Sanders, and Harambe the gorilla were posted. The Texas Department of Transportation responded to the hacked message boards saying they belonged to a private contractor who was investigating how they might have been hacked.⁴



Figure 13. The hacked traffic message sign

(Source: <https://twitter.com/CBSDFW/status/739453948633845761>)

- November 26, 2016. The San Francisco Examiner reported that the San Francisco Municipal Transportation agency (Muni) was hit with a crypto-ransomware attack, which displayed the hacker's message on their systems. The message mentioned an email address that has been linked to attacks with malware variants such as HDDCryptor.^{5, 6} Along with this message, fare payment machines at Muni underground stations displayed "OUT OF SERVICE" messages. Unable to charge its customers, Muni allowed free rides on its light-rail vehicles.⁷



Figure 14. The compromised automated fare payment systems

(Source: <http://www.sfexaminer.com/hacked-appears-muni-stations-fare-payment-system-crashes>)

- January 27, 2017. The Washington Post reported that 70% of the storage devices that record data from D.C. police surveillance cameras were infected with ransomware by hackers eight days before President Donald Trump's inauguration. The ransomware left the local police unable to record between January 12 to 15, with the attack affecting 123 of 187 network video recorders.⁸



Figure 15. DCPD police car

(Source: <https://cdn2.img.sputniknews.com/images/105598/15/1055981593.jpg>)

- April 9, 2017. CNN reported that hackers set off all 156 emergency sirens in Dallas around 11:40 p.m.⁹ The emergency sirens used radio communication only, with no internet connection between the control center and the siren units. The hackers manipulated the radio communications to gain control privileges and trigger the sirens. While this was not a direct cyberattack against ITS infrastructure, Dallas residents calling 911 clogged the emergency systems for hours.¹⁰ This in turn would have directly affected emergency vehicle management systems.



Figure 16. Emergency sirens in Dallas

(Source: <https://www.gizmodo.com.au/2017/04/156-hacked-emergency-sirens-show-dallas-officials-that-they-have-a-security-problem/>)

- April 21, 2017. RP Online reported that a planned system upgrade of Rheinbahn's (public transit company in Düsseldorf, Germany) routing and scheduling system went horribly wrong and resulted in extensive delays and cancellations of bus and train services, causing public suffering. A total of 832 vehicles on more than 80 routes were affected because of the failed system upgrade. Drivers had to revert to displaying handwritten signs on the front of the buses and trains because the digital signs were displaying incorrect information. While this was not an ITS cyberattack, it clearly demonstrates that these types of incidents can have equally adverse consequences.¹¹



Figure 17. Rheinbahn transportation network hacked into a standstill

(Source: <https://www.report-d.de/Duesseldorf/Verkehr/Duesseldorf-zwischen-Update-und-Absturz-Schwarzer-Donnerstag-bei-der-Rheinbahn-Tausende-kamen-zu-spaet-75475>)

- May 13, 2017. Radio Liberty reported that Russian Railways computers were infected by the WannaCry ransomware. WannaCry infected more than 200,000 computers in 150 countries within a day of the initial outbreak.^{12 13} Russian Railways confirmed that the infection was localized and rail transportation was not affected. The Telegraph reports that WannaCry infected German train stations, and passenger information monitors were seen displaying the ransom window. Deutsche Bahn said, "Due to a Trojan attack there are system failures in various areas".¹⁴ WannaCry is a ransomware that exploits an SMB vulnerability (MS17-010) to spread and infect unpatched systems and demands a \$300 ransom in bitcoins for decryption. If no payment is received in a week's time, then all the encrypted files on the system will be deleted. Any organization running unpatched or older versions of Windows can become victims of WannaCry.¹⁵



Figure 18. WannaCry infection at Deutsche Bahn Train Station

(Source: <http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/>)

- May 17, 2017. USA Today reported that information display screens at the Washington, D.C. Union Station were hacked and started playing video from Pornhub during rush hour. The monitors were quickly turned off. The authorities have not shared further details about this security breach incident.¹⁶



Figure 19. Hacked Video ad screen at Union Station

(Source: <http://www.nbcwashington.com/news/local/Porn-Aired-on-Video-Ad-Screen-at-Union-Station-422592524.html>)

- July 26, 2017. Motherboard reported that security researchers have found vulnerabilities in internet-connected drive-through car washes that can let hackers remotely hijack the system and physically attack vehicles and their occupants. The hackers can take control of the bay doors and use them to strike vehicles entering/exiting the car wash or trap vehicles inside the car wash, and in the process damage vehicles and hurt occupants. While car washes are not integrated into ITS and hacked car washes would realistically cause limited damage before discovery, we still included this in the real-world attacks list because vehicle and driver safety may be jeopardized by a compromised internet-connected system.¹⁷



Figure 20. Internet-connected automatic car wash

(Source: <https://tiresandparts.net/news/parts/automatic-car-washes-vulnerable-hacking/>)

- August 4, 2017. Autoblog reported that a group of university researchers have figured out how to hack self-driving cars by putting stickers on street signs. The researchers analyzed image classification algorithms used by vision systems in self-driving cars, and then visually manipulated street signs using stickers in order to trick the machine-learning models into misinterpreting them. In one example, they used stickers to trick the vision system of an autonomous car into reading a STOP sign as a 45-miles-per-hour sign instead. The consequences of such simple attacks can be devastating in the real world, especially now that we have semi-autonomous driving capabilities in many road vehicles.¹⁸



Figure 21. Stickers used to visually manipulate street signs and confuse autonomous cars

(Source: <https://www.autoblog.com/2017/08/04/self-driving-car-sign-hack-stickers/>)

- August 4-7, 2017. Multiple incidents of hacked highway message boards in California were reported. Offensive messages posted include: “Trump has herpes,” “free hookers ahead,” and “Caution Asian drivers.” In one incident the electronic message board was secured using a password, but hackers still managed to bypass the password and post their message. While these may be pranks, they can distract drivers and jeopardize road safety.^{19, 20}



Figure 22. The hacked highway message board sign

(Source: <http://fox40.com/2017/08/03/road-sign-in-solano-county-hacked-to-say-trump-has-herpes/>)

While some of the incidents listed here can be attributed to simple vandalism, the fact remains that ITS technology is vulnerable to such attacks and can draw attention from cybercriminals hoping to exploit the systems.

Legislation is already being drafted to mandate V2V & V2I communications. Once those legislations pass and standards are developed, interconnection will happen rapidly. Autonomous vehicles are currently in the early development stages, but progress is being made rapidly as big investments are pouring in to make autonomous vehicles roadway reality. ITS will clearly have to contend with cyberattacks as complete integration and interconnection are slowly achieved. This stresses the importance of securing ITS at the beginning. After all, ITS will not only have an impact on economic gains but on public safety as well.

ITS Attackers

Where there are opportunities, there are also perpetrators who attack, leverage, steal, game, and abuse the system for a wide variety of reasons, such as money, revenge, and protest. In this section we discuss the different types of perpetrators who pose threats to ITS infrastructure.

- **Nation States** — Both developed and developing countries gather intelligence using software espionage tools and customized malware. Based on our observation of current cyberattacks, the primary goal for state-sponsored attacks is to steal intellectual property or to gain competitive advantage. But in certain instances, for example, during a war, one nation can sabotage another nation's ITS infrastructure. State-sponsored attacks follow one of two *modi operandi*. It's either the state directly controls the hacking teams and their resources, or the state outsources the hacking activities to third parties such as criminal gangs to maintain plausible deniability.
- **Criminal Gangs** — Highly skilled hacking teams, funded and controlled by organized criminal gangs, target victims using different schemes such as ransomware, phishing, drive-by-download, etc., to generate illicit revenue for the gangs. There are also criminal hacking groups who are contracted by national governments for various political cyberattacks, including cyber espionage and subterfuge.
- **Hacktivists** — Internet activists who attack cyber assets to draw attention to their political causes and tend to choose highly visible, high-profile targets. ITS infrastructure such as highway digital message boards are frequent targets of hacktivists protesting causes such as the environment, politics, corporate greed, and the like.
- **Cyberterrorists** — Their goal is to launch disruptive or destructive cyberattacks to cause physical destruction of property or loss of life, as well as spread terror.
- **Insiders** — Insider motives can be tricky to decipher. They act against organizations that they are or were part of and indirectly act against their own interests. Insiders could be motivated by money, ideology, coercion, ego, revenge, and politics. More than one of these motives are usually at play in an attack levied by an insider.

- **Unscrupulous Operators** — The primary users of ITS infrastructure are the drivers on the roads. This includes both regular drivers and commercial vehicle operators. It's not inconceivable to imagine scenarios where drivers and commercial operators try to hack and game the system to save on fines and fees, to get ahead in traffic, do competitor sabotage, etc.
- **Natural Disasters** — Snow, rain, high winds, and other natural phenomena can cause system failures that effectively cripple ITS infrastructure. One example is Vancouver's fully autonomous Skytrain system slowing or shutting down whenever there is heavy snowfall in the region, due to the resulting snow and ice tripping the intrusion sensors on the Skytrain's exposed tracks. This stops the trains from running.²¹ Skytrain's solution is to manually run the trains during heavy snow, which in itself is a slow process.

Aside from natural disasters and roadway users, we can see that the usual suspects of ITS cyberattacks are not different from the everyday perpetrators who launch cyberattacks against the online systems of organizations, governments, and critical infrastructure. While this might make it seem like securing ITS infrastructure is easy, in reality it is far from simple. The ITS ecosystem is constantly evolving and so are the threats. It is not unreasonable to imagine that, in the future, new perpetrators will emerge who we do not identify as a threat today, such as artificial intelligence actors.

ITS Attacker Motives

From the perpetrators themselves, we next examine their motives. The key motivator for the vast majority of cyberattacks that we see daily is: Money. But in the ITS world, not every perpetrator that will attack the ITS ecosystem will be motivated by money. ITS systems are highly visible and attacks against them will be high impact. That itself is a key motivator for many of the perpetrators. We have identified five broad objectives and profiteering models that motivate perpetrators to attack the ITS ecosystem.

Objectives & Profiteering Models	Impact
Ransom	<p>Attackers can encrypt data and systems and demand a ransom payment to release decryption key(s). This will severely impact daily ITS operations, hurt revenue generation streams, affect the company's credibility, and potentially shut down critical systems responsible for public safety. Poorly designed ransomware malware can also irreversibly corrupt data and systems, making recovery impossible even with the decryption keys.</p> <p>In the future, it is expected that perpetrators will devise methods of sending malicious firmware upgrades over-the-air (OTA) to connected cars, and disable the car's functions until the owner pays the demanded ransom. An OTA ransomware attack that happens while the connected car is traveling on the road will severely impact the safety of the vehicle's passenger(s) and other vehicles on the road.</p>
Data Theft	<p>Perpetrators can steal proprietary data, intellectual property, business operations data, personally identifiable information (PII), financial data, sales data, customer information, shipment data, vehicle tracking information, etc. and monetize the stolen data in various ways. The stolen data can be used for identity theft, privacy violation, financial fraud, industrial espionage, and other crimes/threats related to information theft.</p> <p>Two of the most likely perpetrators who steal data are nation states and unscrupulous competitors. Their goals include (but are not limited to) gaining competitive advantage especially in contract bidding, copying expensive research, identifying operational weaknesses, improving their own business processes, etc.</p>

Objectives & Profiteering Models	Impact
Information Warfare	<p>This is a broad topic that encompasses everything from hacktivism to information pollution for financial gains. Some of the information attacks that we've identified are as follows:</p> <ul style="list-style-type: none"> • Launching a distributed denial-of-service attack (DDoS) against ITS infrastructure to crash the systems and cause roadway chaos. • Hacking company apps or websites to post political, protest, or prank messages. Another agenda could be to hurt the ITS company's reputation and cause them financial losses. • Hacking dynamic message signs on roadways to post political, protest, or prank messages. • When cooperative autonomous vehicles become roadway reality, criminals may be able to transmit fake V2V messages to create traffic chaos. • V2V information poisoning can become a service where unscrupulous businesses will pay criminals to poison V2V channels and force-reroute autonomous vehicles to their business locations. • Map hacking (done via compromising road-based location transmitters, hacking on-board GPS receivers, or GPS signal spoofing) can cause autonomous vehicles to veer off-course and cause an accident.

Objectives & Profiteering Models	Impact
System Gaming and Theft	<p>One of the most attractive profiteering models for perpetrators would be to steal goods or valuables inside the vehicles, or the vehicles themselves. Others may try to exploit ITS systems to avoid paying service charges. We identified the following attacks:</p> <ul style="list-style-type: none"> • Hacking and rerouting autonomous trucks to some remote location (e.g., an empty parking lot outside town), where the criminals can break into the trucks and steal the cargo inside. • Using hacked autonomous vehicles to anonymously deliver contraband such as drugs and weapons. • Hacking autonomous passenger vehicles and instructing them to reroute and stop at some obscure location. The criminal's goal is to steal the passengers' valuables, or even abduct someone. • Hacking autonomous vehicles, and rerouting and stopping them to steal vehicle parts or the vehicles themselves. • Exploiting compromised ITS systems to avoid paying service charges, e.g., parking, bridge tolls, congestion charges, etc. • Mobile Infrared Transmitter (MIRT) devices can remotely change computer-controlled traffic lights that have built-in preemption receivers.²² In the future there may be sophisticated MIRT-style devices that can disrupt traffic flow in favor of the device owner. • Unscrupulous ITS service providers (e.g., autonomous taxi and delivery service providers) may attempt to subvert competition by hacking their competitors' autonomous vehicles and making them unavailable. • Illegally assigning higher priority to an autonomous vehicle on a dedicated roadway so other autonomous vehicles move aside. • Making fake orders of autonomous vehicle rideshares to charge unsuspecting customers.

Objectives & Profiteering Models	Impact
Revenge and Terrorism	<p>Terrorist attacks where the attacker drives into innocent people and kills them have recently been making disturbing news headlines around the world. In an ITS ecosystem complete with autonomous vehicles, terrorist attacks using the autonomous vehicles remains one of the most serious and deadly attack vectors that we need to protect against.</p> <p>If the driving functions of autonomous vehicles can be compromised, then there is every possibility that the vehicles may be used as weapons in terror attacks. Terror attacks primarily target people, but we surmise that hijacked vehicles can also be used for attacking critical infrastructure. The terrorists can launch these attacks remotely, which makes tracking the attackers extremely difficult, if not impossible.</p> <p>The Bridgegate scandal, which made headlines in the United States, was motivated by political revenge. Staffers behind the decision to close traffic lanes on the George Washington Bridge without any prior public notifications, as stipulated by the law, were later convicted by the courts.²³ The incident shows that insider and revenge attacks are a reality, and they are very difficult to predict and defend against. These are some likely attack scenarios we identified:</p> <ul style="list-style-type: none"> • Deliberately disrupting traffic by manipulating traffic flow control mechanisms like road barriers, lane signals, traffic lights, etc. The end goal is to create chaos on the roadways or, in extremes cases, cause accidents. • Disabling critical ITS safety systems and thereby jeopardizing public safety. This will affect all modes of transportation that relies on the ITS safety systems for safe travel on the roadways. • Triggering roadside emergency alert systems, e.g., tornado warning sirens. • Dumping sensitive data online that compromises the company's operations and the privacy of its employees.

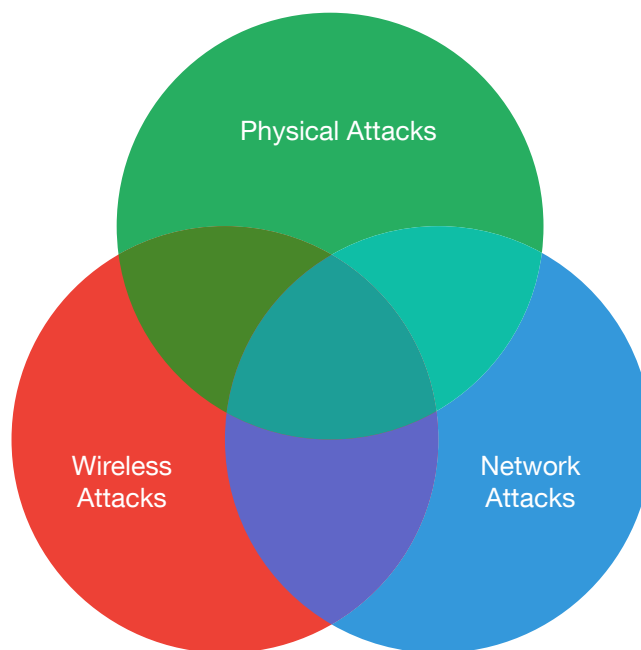
From a cybersecurity perspective, one glaringly obvious reason for hacking ITS systems is to use them as an entry point into the greater ITS ecosystem. ITS systems installed on the roadways are physically accessible to just about anyone, and they are connected via the internet or via virtual private networks (VPN) to the ITS ecosystem. If an attacker can successfully exploit the ITS system to gain access into the corporate network, then they can penetrate deep inside the network with minimal effort since the ITS system is considered a trusted node. Once inside the network, the perpetrators can launch any of the attacks that we just described.

ITS Attack Vectors

ITS is a massive, complex, interconnected ecosystem with millions of endpoints and end users. The size, complexity, and functions of this ecosystem create large and at times unpredictable attack surfaces. Many of the attack vectors against ITS fall outside the scope of this paper; therefore, we only focused on attack vectors that result in the compromise and/or abuse of ITS devices and systems.

ITS Attack Vectors

After much analysis, we've sorted ITS attack vectors into three broad overlapping categories: physical, wireless, and network attack vectors.



The overlap between each category of attacks represents how the attack vectors can fluidly transition from one category to the next, or how different categories of attacks can be chained together to successfully compromise the ITS devices and systems.

Attack Category	Methods
Physical Attacks	<p>ITS infrastructure sits physically exposed on roadways and roadsides, making them accessible to anyone who walks up to them. Attack vectors which abuse ITS ease-of-physical-access include:</p> <ul style="list-style-type: none"> • Physically connecting to exposed ports, e.g., USB, PS2, serial, etc. • Using brute force or guessing credentials on a device • Sniffing network traffic between a device and the backend • Scanning the secured/closed network to discover topology • Deleting files on the compromised ITS device/system • Dumping firmware to recover credentials and configuration • Man-in-the-Middle (MitM) attacks using exposed wires/cables to intercept data • Physically tampering with a device to steal/compromise data, modifying a device, etc. • Connecting a removable storage device loaded with malware to install • Sending improper commands to the controller and backend servers • MitM attack communications and sending false data to backend servers • Pivoting an ITS device as a trusted entry point into the corporate network • Exploiting vulnerabilities in software, hardware, protocols, OS, etc. • Abuse of authority by trusted operators to tamper with and compromise devices

Attack Category	Methods
Wireless Attacks	<p>V2V, V2I, and I2I wireless communications will form the backbone of future ITS operations. Wirelessly hacking ITS infrastructure will pose a major IT security challenge for ITS operators. Attack vectors that leverage wireless transmissions include:</p> <ul style="list-style-type: none"> • Spoofing V2V, V2I, and I2I messages broadcast to traffic and the rest of the ITS ecosystem • Sniffing wireless transmissions, e.g., using the car's Wi-Fi²⁴ • Remotely transmitting and installing malicious firmware • Electronic jamming of wireless transmissions to disrupt operations • MitM attack with wireless transmission to intercept and/or modify data • Exploiting vulnerabilities in software, hardware, protocols, OS, etc. • Using vehicle Wi-Fi as an entry point into the controller area network (CAN) bus and then to the on-board diagnostics (OBD), telematics control unit (TCU), and in-vehicle infotainment (IVI) • Remote hijacking of vehicle controls via compromised CAN bus • Installing malicious third party apps in a car's infotainment system • Attacking via malicious app installed on a phone connected to the car's Wi-Fi • Electronic jamming of vehicle's safety systems, e.g., radar, ultrasonic sensors, etc.

Attack Category	Methods
Network Attacks	<p>We are now in the traditional IT security space where the vast majority of cyberattacks against systems can originate over the network. Internet-exposed ITS systems, discoverable via IoT search engines such as Shodan, are particularly vulnerable to cyberattacks. Traditional network-based attack vectors include:</p> <ul style="list-style-type: none"> • Identifying and abusing device misconfigurations • Exploiting vulnerabilities in legacy software and hardware • Remote system discovery and abuse, e.g., discovery using Shodan • Installing malware/spyware on systems • Sophisticated state-sponsored targeted attacks or advanced persistent threats (APTs) • Uploading and installing malicious firmware • Social engineering attacks, e.g., spear-phishing • Launching DDoS attacks on internet-exposed ITS infrastructure and backend servers • Exploiting vulnerabilities in software, hardware, protocols, OS, etc. • Credential brute forcing and abusing weak authentication mechanisms • Malicious script injection via ads, banners, malvertising, etc. • SQL injection attacks • Cross-site scripting (XSS) attacks • Session hijacking attacks • DNS spoofing and hijacking attacks • Watering hole attacks • Pass the Hash attacks • Pass the Ticket attacks (Kerberos) • Sending improper commands to the controller and backend servers • Pivoting an ITS device as a trusted entry point into the corporate network • Abuse of authority by trusted operators to compromise systems/devices • Compromising a third-party contractor's computers and accessing the corporate network via those infected machines

It is very possible that a singular attack can involve all three attack categories at the same time. For example, in an attack against a traffic flow controller device such as Dynamic Message Signs (DMS), the attackers can send the device incorrect/improper commands via a wireless link, by physically connecting to the device, and/or over the network using a compromised controller application. The nature and functionality of DMS make this attack vector multimodal.

Attacks Against VANETs

Connected vehicles, and in the future autonomous vehicles, will become the primary roadway users. One of the key technologies connected vehicles will use is: Vehicular Ad hoc Networks (VANETs). VANETs are comprised of smart vehicles and Roadside Units (RSU) which communicate through unreliable wireless media. Because of their ad hoc nature, VANETs are susceptible to attacks that can jeopardize roadway safety, especially when vehicles depend on VANET data for making critical driving decisions. We summarized the VANET attack vectors described by Fatih Sakiz and Sevil Sen in their paper, “A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV.”²⁵

- **Sybil Attack** — In which a node (vehicle) pretends to have more than one identity. The result is other vehicles in the network cannot verify if the received data originates from one vehicle or multiple vehicles. The aim of the attacker is to shape the network based on their goals. Sybil attacks are considered one of the most dangerous attacks against VANETs and are very difficult to detect.
- **DDoS Attack** — In which one overwhelms a system with more requests than it is designed to handle. This causes the targeted system to crash or become unavailable. In VANETs, attackers could try to shut down the network established by RSUs and stop communications between vehicles and/or RSUs.
- **Blackhole Attack** — In which the attacker node in an ad hoc cooperative network manipulates other nodes into routing their data packets through the attacker. The attacker then intentionally discards the data packets, resulting in communication loss in the network and other vehicles not receiving crucial roadway information.
- **Wormhole Attack** — In which two or more compromised nodes involve themselves in as many routing requests as possible by falsely advertising that they know the shortest path to any destination. The goal of the attackers is to modify the logical topology of the network and route all routing requests through themselves in order to collect and/or manipulate large amounts of network traffic.
- **False Information Attack** — In which VANETs vehicles use data generated or forwarded by other vehicles or RSUs. The received/forwarded data may not be true; an attacker vehicle can generate false data and send it to the VANET. Common false information attacks include:

- **Fake Location Information** — Vehicles can broadcast fake location data. This is a serious problem because safety-related applications/systems that rely on accurate vehicle location data will respond incorrectly. Also, false location information will result in data packet loss, as packets will be forwarded to phantom vehicles.
- **Sensor Deception** — By simulating false driving conditions, attackers can deceive in-vehicle sensors, e.g., by braking repeatedly over a short distance, the attacker can simulate a traffic jam on the road, and the car can incorrectly broadcast a traffic jam message.
- **Replay Attack** — In which messages are stored and broadcast later in order to deceive other nodes in the network. In a replay attack, the message that is replayed is no longer valid or true. The aim of the attack is to recreate and exploit the conditions at the time the original message was sent by rebroadcasting the stored message.
- **Passive Eavesdropping Attack** — Refers to monitoring the network to track vehicle movement or to listen to their communications. The attacker node simply intercepts and examines the messages that flow through the network. The attacker's goal is to gather information about the vehicles and their communication patterns for use in future attacks.

Internet-Exposed ITS Devices

The abuse and compromise of internet-exposed ITS infrastructure kept on reappearing in our analysis. Internet-exposed ITS systems, which we define as discoverable via IoT search engines like Shodan, are vulnerable to everyday cyberattacks such as distributed denial-of-service (DDoS) attacks. We put the theory to the test and attempted to discover internet-exposed ITS infrastructure in Shodan.

We searched for the term “NTCIP” (short for National Transportation Communications for Intelligent Transportation System Protocol) in Shodan and discovered 63 NTCIP compliant devices exposed online in the U.S. The devices discovered were either Econolite® ASC/3 traffic light controllers, or Skyline Dynamic Message Signs (DMS) controllers. These controllers were connected to the internet via wireless modems. The organization names listed are those of the ISPs who provide the wireless modems and NOT the operators who own/operate the controllers. We note: **No vulnerabilities were discovered in Econolite or Skyline products**. Rather, the operators have configured their controllers to be accessible via the internet. We have removed the IP addresses and hostnames in the screenshots for privacy reasons.

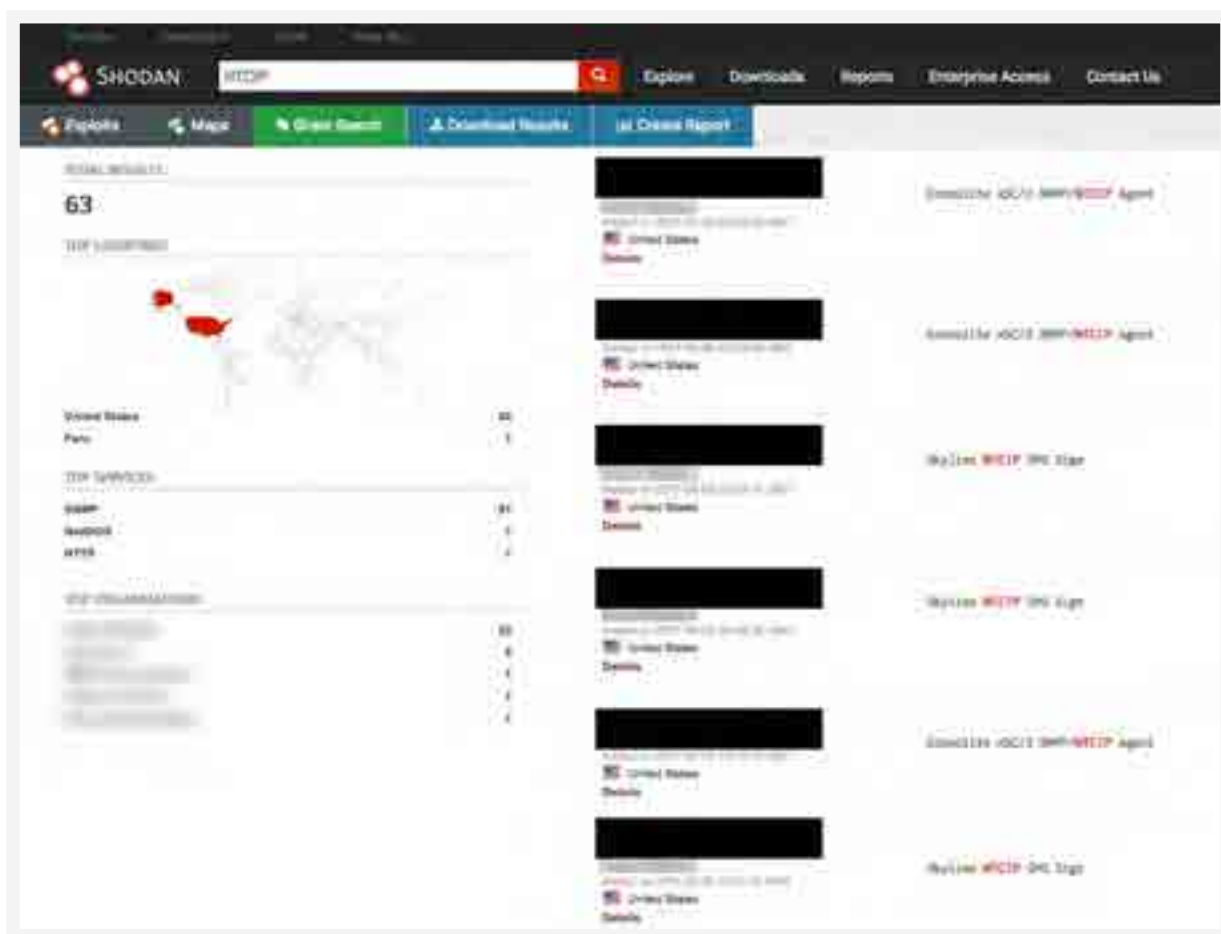


Figure 23. Internet-exposed Econolite ASC/3 traffic light controllers and Skyline DMS controllers



Figure 24. Controller connected to the internet using a 4G wireless modem

A well-known research paper from 2014 discussed how vulnerable traffic signal controllers are. The researchers from the University of Michigan’s EE/Computer Science Department “found three major weaknesses in the traffic light system: unencrypted wireless connections, the use of default usernames and passwords that could be found online, and a debugging port that is easy to attack”.²⁶ Once a traffic light is hacked, attackers can alter the light timing or permanently freeze them in one state.²⁷ If traffic signals are now connected to the internet via wireless modems and discoverable using an IoT search engine like Shodan, then the risk factor of the signals getting hacked/compromised exponentially increases.

Encouraged by easily discovering NTCIP-compliant devices exposed online, we decided to search Shodan with the names of different ITS device manufacturers. We searched for Daktronics, a popular manufacturer of DMS, and found more than 200 instances of Daktronics VFC-3000 Vanguard® VMS Field Controllers exposed online in Canada and the U.S. Like with NTCIP-compliant devices, these controllers were also connected to the internet via wireless modems. The organization names listed are those of the ISPs who provide the wireless modems and NOT the authorities/operators who own/operate the controllers. Likewise, **no vulnerabilities were discovered in Daktronics products**. It was the operators who configured their controllers to be accessible via the internet. We have removed the IP addresses and hostnames in the screenshots for privacy reasons.

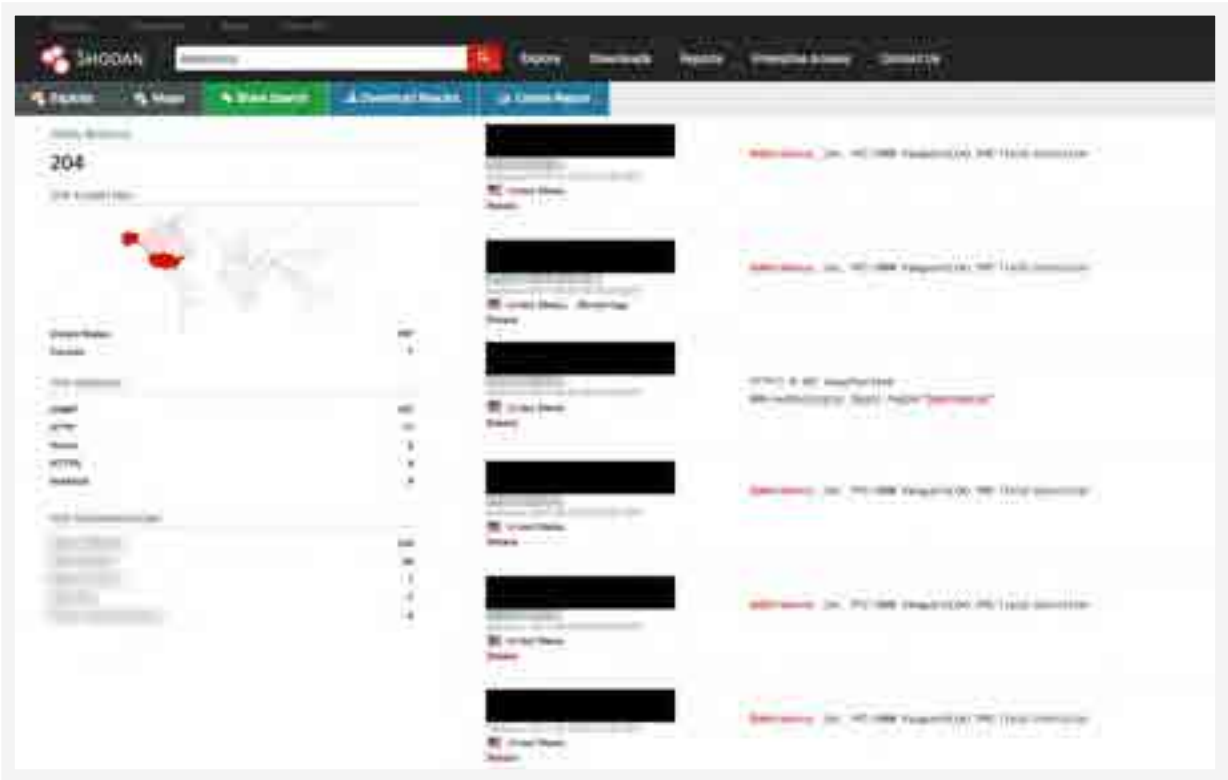


Figure 25. Internet-exposed Daktronics VFC-3000 Vanguard VMS Field Controllers

We also searched for Wanco, a popular manufacturer of highway safety and traffic control products. We found 89 instances of Wanco Message Board exposed online in the U.S. Similar to our previous findings, these devices were connected to the internet via wireless modems. What is worrisome is that some of the wireless modems connecting the Wanco Message Boards to the internet were running Allegro RomPager v4.01. RomPager v4.34 and older versions are known to be exploitable by the vulnerability called “Misfortune Cookie” (CVE-2014-9222).²⁸ Note that the organization names listed are those of the ISPs who provide the wireless modems and NOT the authorities/operators who own/operate the controllers. **No vulnerabilities were discovered in Wanco products.** But if the RomPager vulnerability is not patched in the wireless modems, then it opens up the possibility of device compromise by perpetrators via the modem.

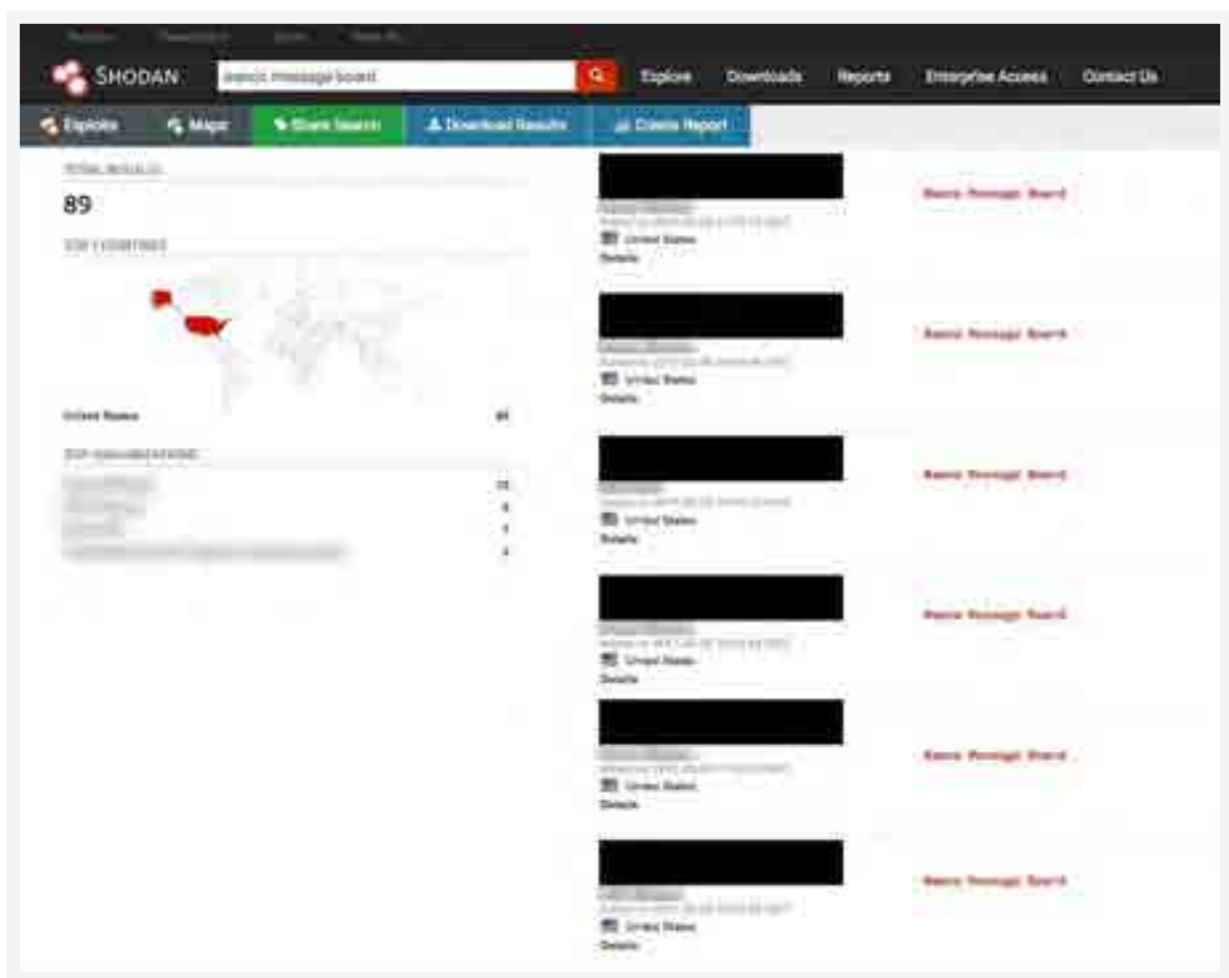


Figure 26. Internet-exposed Wanco Message Board controllers



Figure 27. Controller-connected to the internet using a wireless modem running Allegro RomPager v4.01

An internet-exposed device doesn't mean the system was compromised, but rather that it was not configured to be secure. On the flipside, by virtue of being exposed on the internet, the system is vulnerable to compromise. We also find that perpetrators can exploit known vulnerabilities in the wireless modem to potentially access and compromise the connected ITS devices. For an in-depth discussion on router/modem vulnerabilities and the risks of internet-exposed devices, refer to the Trend Micro research papers "Securing Your Home Routers — Understanding Attacks and Defense Strategies"²⁹ and "US Cities Exposed — A Shodan-Based Study of Exposed Assets in the US"³⁰.

Threat Modeling the ITS Ecosystem

In the previous section, we discussed the different ITS cyberattack vectors. In this section, we disseminate the cyberattack vectors across six ITS applications and systems (introduced earlier) and apply the industry-standard DREAD threat model to calculate the risk ratings of these attacks. Threat modeling, in a nutshell, is a form of risk assessment that models aspects of attack and defense sides of a system, environment, etc.³¹

Categorizing ITS by Impact Severity Levels

As mentioned previously, ITS is a massive ecosystem with many working components, each serving a different function. For the purpose of threat modeling, we grouped these components according to an Impact Severity Level (ISL) that we defined to calculate their overall risk ratings. We defined the following ISLs:

- L1 — Applications and systems that directly affect public safety and critical operations.
- L2 — Applications and systems that affect daily operations and revenue generation.
- L3 — Applications and systems that support L1, L2, and the organization itself.

The ITS components are described in detail in the Appendix.

ITS Category	L1	L2	L3
Vehicles	GPS; RADAR; LIDAR; ultrasonic sensors; stereovision cameras; Lane Keep Assist; infrared sensors; telematics & OTA services; V2V & V2I		

ITS Category	L1	L2	L3
Roadway Reporting	Induction loops; vehicle detection systems; roadside weather stations	Bus lane cameras; HOV lane cameras; red-light cameras; speed cameras; railway crossing cameras; ANPR; UAV road monitoring; vehicle location tracking	Emissions/Air quality sensors
Traffic Flow Controls	Reversible lanes; railway crossing barriers; Dynamic message signs; dynamic road surface markers; dynamic road barriers; traffic signal control systems; ramp meters; pedestrian detectors; bicyclist detectors; emergency vehicle priority systems; transit signal priority; safety systems for autonomous vehicles; dedicated lanes for autonomous vehicles	Dynamic message signs; automated toll collection systems	
Payment Applications and Systems		RFID payments; kiosk payments; ticket payments; app payments; ANPR automatic payments; dynamic tolling; congestion zone charges; parkade payments; roadside parking payments; freight truck tolls; multimodal transportation payments	
Management Applications and Systems	Street light controls; disaster management; transit vehicle management; emergency vehicle management; traffic & congestion management; smart traffic light controller systems; road-based location services for autonomous vehicles	Information sharing services; data management & storage systems; smart parking management; billing & tolling administration; commercial vehicle operations; maintenance & construction management	Cooperative traffic & position sharing; artificial intelligence & machine learning applications

ITS Category	L1	L2	L3
Communications Applications and Systems	Road obstacles & accident alerts; telematics & eCall; emergency vehicle warning systems; road information displays & alert systems; communication cell towers, antennas, & repeaters; I2I, V2V, & V2I communications	Smart apps; company website; advertisements; passenger travel information	Smart apps; social media; company website

It is not at all surprising to find that the majority of ITS systems are classified as L1. This is because these systems play a critical role in moving vehicle traffic safely and efficiently.

The DREAD Threat Model

Threat modeling allows us to apply a structured approach to security and to address the top threats that have the greatest potential impact on the application.³² Qualitative risk analysis is opinion based; it uses rating values to evaluate the risk level. The industry-standard DREAD threat model can be used for such a purpose.³³ We arrived at the risk rating for a given threat by asking the following questions^{34 35}:

- **Damage potential** — How great is the damage to the assets?
- **Reproducibility** — How easy is it to reproduce the attack?
- **Exploitability** — How easy is it to launch an attack?
- **Affected users** — As a rough percentage, how many users are affected?
- **Discoverability** — How easy is it to discover this threat?

We created the following threat rating table for our ITS risk analysis.

Rating		High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker subverts the system and can inflict serious damage.	The attacker subverts the system and can inflict moderate damage.	The attacker subverts the system and can inflict minor damage.
R	Reproducibility	The attack can be reproduced every time.	The attack can be reproduced, but only within set limitations.	The attack is very difficult to reproduce, even with full knowledge of the security hole.
E	Exploitability	The attack requires little or no knowledge of the system in order to exploit it.	The attack requires a skilled operator with fundamental knowledge of the system in order to exploit it.	The attack requires an extremely skilled operator with in-depth knowledge of the system in order to exploit it.
A	Affected users	Majority of the everyday users will be affected by the attack.	A good-sized portion of everyday users will be affected by the attack.	A very small percentage of everyday users will be affected by the attack.
D	Discoverability	Published information readily explains the attack. Vulnerabilities are found in the most commonly used applications and systems.	Vulnerabilities are not common and only found in certain applications and systems. It requires skills to weaponize vulnerabilities.	Extremely difficult to discover vulnerabilities, and they are very difficult to weaponize.

After answering the DREAD questions for a given threat, the risk rating is calculated by adding the rating values. The overall risk is rated as follows:

- **High Risk** if the score is between: [12 – 15]
- **Medium Risk** if the score is between: [8 – 11]
- **Low Risk** if the score is between: [5 – 7]

Measuring the Risk of Attacks Against ITS

For each of the six ITS categories, we selected five cyberattack vectors that are most likely to strike ITS applications and systems. We then assigned scores for realistic extreme scenarios to the cyberattack vectors and calculated the risk rating using the DREAD threat model.

ITS Category : Vehicles (NET = Network Attack; PHY = Physical Attack; WIR = Wireless Attack)

Attack Vectors	ISL	D	R	E	A	D	Rating
Spoofed V2V and V2I messages broadcast (WIR)	L1	3	2	1	2	2	Medium
	L2						
	L3						
Malicious firmware uploaded and installed via OTA service (WIR)	L1	3	1	1	1	1	Low
	L2						
	L3						
Electronic jamming of wireless transmissions to disrupt operations, and/or jam safety systems, e.g., RADAR, ultrasonic sensors, etc. (WIR)	L1	3	2	3	1	3	High
	L2						
	L3						
Remote hijacking of vehicle controls (WIR)	L1	3	2	1	1	2	Medium
	L2						
	L3						
Malicious third-party app installed in car's in-vehicle infotainment system (WIR)	L1	3	3	2	3	2	High
	L2						
	L3						

ITS Category: Roadway Reporting (NET = Network Attack; PHY = Physical Attack; WIR = Wireless Attack)

Attack Vectors	ISL	D	R	E	A	D	Rating
Electronic jamming of wireless transmissions to disrupt operations (WIR)	L1	3	2	3	2	3	High
	L2	3	2	3	2	3	High
	L3	3	2	3	1	3	High
Physically tampering with device to install malware, modify device, steal data, etc. (PHY)	L1	3	2	2	2	2	Medium
	L2	3	2	2	2	2	Medium
	L3	3	2	2	1	2	Medium
DDoS internet-exposed devices and systems (NET)	L1	3	3	3	2	3	High
	L2	3	3	3	2	3	High
	L3	3	3	3	1	3	High
Using compromised ITS device as entry point into corporate network (NET or PHY)	L1	2	1	2	1	2	Medium
	L2	2	1	2	1	2	Medium
	L3	2	1	2	1	2	Medium
Sending improper commands to the controller and backend servers (NET or PHY or WIR)	L1	3	1	1	2	2	Medium
	L2	3	1	1	2	2	Medium
	L3	3	1	1	1	2	Medium

ITS Category: Traffic Flow Controls (NET = Network Attack; PHY = Physical Attack; WIR = Wireless Attack)

Attack Vectors	ISL	D	R	E	A	D	Rating
Sending improper commands to the controller and backend servers (NET or PHY or WIR)	L1	3	1	1	3	2	Medium
	L2	3	1	1	3	2	Medium
	L3						
DDoS internet-exposed devices & systems (NET)	L1	3	3	3	3	3	High
	L2	3	3	3	3	3	High
	L3						
Physically tampering with device to install malware, modify device, steal data, etc. (PHY)	L1	3	2	2	3	2	High
	L2	3	2	2	3	2	High
	L3						
Electronic jamming of wireless transmissions to disrupt operations (WIR)	L1	3	2	3	3	3	High
	L2	3	2	3	3	3	High
	L3						
Exploiting vulnerabilities in hardware, software, OS, protocol, etc. (PHY or NET or WIR)	L1	3	2	2	3	2	High
	L2	3	2	2	3	2	High
	L3						

ITS Category: Payment A&S (NET = Network Attack; PHY = Physical Attack; WIR = Wireless Attack)

Attack Vectors	ISL	D	R	E	A	D	Rating
Installing malware to disrupt operations and/or steal data (NET)	L1						
	L2	3	2	2	3	2	High
	L3						
DDoS internet-exposed devices and systems (NET)	L1						
	L2	3	3	3	3	3	High
	L3						
Using compromised ITS device as entry point into corporate network (NET)	L1						
	L2	2	2	2	1	2	Medium
	L3						
Exploiting vulnerabilities in hardware, software, OS, protocol, etc. (NET)	L1						
	L2	3	2	2	3	2	High
	L3						
Credential brute forcing and abusing weak authentication mechanisms (NET)	L1						
	L2	3	3	3	3	3	High
	L3						

ITS Category: Management A&S (NET = Network Attack; PHY = Physical Attack; WIR = Wireless Attack)

Attack Vectors	ISL	D	R	E	A	D	Rating
Installing malware to disrupt operations and/or steal data (NET)	L1	3	2	2	3	2	High
	L2	3	2	2	2	2	Medium
	L3	3	2	2	1	2	Medium
Credential brute forcing and abusing weak authentication mechanisms (NET)	L1	3	3	3	3	3	High
	L2	3	3	3	2	3	High
	L3	3	3	3	1	3	High
DDoS internet-exposed devices and systems (NET)	L1	3	3	3	3	3	High
	L2	3	3	3	2	3	High
	L3	3	3	3	1	3	High
Exploiting vulnerabilities in hardware, software, OS, protocol, etc. (NET)	L1	3	2	2	3	2	High
	L2	3	2	2	2	2	Medium
	L3	3	2	2	1	2	Medium
Sending improper commands to the controller and backend servers (NET)	L1	3	1	1	3	2	Medium
	L2	3	1	1	2	2	Medium
	L3	3	1	1	1	2	Medium

ITS Category: Communications A&S (NET = Network Attack; PHY = Physical Attack; WIR = Wireless Attack)

Attack Vectors	ISL	D	R	E	A	D	Rating
Social engineering attacks (NET)	L1	1	1	1	1	1	Low
	L2	3	2	2	2	3	High
	L3	3	2	2	2	3	High
Install malware to disrupt operations and/or steal data (PHY or NET)	L1	3	2	2	3	2	High
	L2	3	2	2	3	2	High
	L3	3	2	2	3	2	High
Send improper commands to the controller and backend servers (PHY or NET or WIR)	L1	3	1	1	3	2	Medium
	L2	3	2	2	3	2	High
	L3	3	2	2	3	2	High
Use compromised ITS device as entry point into corporate network (NET or PHY)	L1	2	1	2	1	2	Medium
	L2	2	2	2	1	2	Medium
	L3	2	2	2	1	2	Medium
Spoofed V2I and I2I message broadcast (NET or WIR)	L1	3	2	1	3	2	Medium
	L2	1		2		2	Low
	L3	1		2		2	Low

Based on the results of our threat modeling exercise, we made the following observations:

- Of the total number of threats that we modeled, 53.85% were rated as High Risk, 40% were rated as Medium Risk, and 6.15% were rated as Low Risk.
- Of the High Risk threats, 71.4% were network attacks (NET), 31.4% were wireless attacks (WIR), and 25.7% were physical attacks (PHY). There are overlaps between NET, WIR, and PHY attacks. The reason for this is that, depending on the nature and functionality of the ITS device/system being attacked, the same attack vector can be PHY, WIR, and/or NET.
- DDoS attacks against exposed cyber infrastructure, electronic jamming of wireless transmissions, vulnerability exploitation, and credential brute forcing attacks all scored as High Risk in the DREAD model. Aside from electronic jamming, the other attack vectors are commonly used in everyday cyberattacks, so it comes as no surprise that attackers will reuse tried-and-tested methods to compromise systems.
- Sensational attacks, such as malicious firmware installed via OTA, remote hijacking of vehicle controls, sending incorrect/improper commands to ITS devices, and sending spoofed V2I and V2V messages, all scored as Medium or Low Risk in the DREAD model. These are difficult attacks to execute because the devices/systems are not readily accessible for attacking, and expert skill and knowledge are required to successfully compromise the devices/systems.
- Surprisingly, leveraging compromised ITS devices/systems as an entry point into the corporate network was assessed to be Medium Risk. This maybe because it requires highly skilled attackers and overcoming corporate IT defenses is hard, thus making attack execution difficult.
- Overall, we discovered that network cyberattacks pose the most serious threat to ITS devices/systems, followed by wireless attacks, and lastly physical attacks.
- Out of the six ITS categories that we threat modeled, Traffic Flow Control systems and Payment Applications and Systems have been found to contain the largest number of threats categorized as High Risk.

Securing the ITS Ecosystem

Protecting the complex ITS ecosystem is a very difficult task, much of which is outside the scope of discussion of this research paper. From our ITS ecosystem threat modeling exercise, we concluded that network cyberattacks pose the most serious threat to ITS, followed by wireless attacks and then physical attacks. Perpetrators targeting ITS include nation states, criminal gangs, hacktivists, terrorists, and insiders who attack ITS infrastructure for a variety of reasons. While it is impossible for this research paper to provide detailed security solutions for every ITS attack scenario, we can discuss broad-spectrum recommendations and security practices to address threats to ITS.

Cyberattack and data breach prevention strategies should be considered an integral part of daily business operations for ITS operators. Ultimately, no defense is impregnable against determined adversaries – cyberattacks and data breaches are inevitable. Therefore, having effective alert, containment, and mitigation processes are critical to the overall protection of an ITS ecosystem.

The key principle of defense is to assume compromise and take countermeasures:

- Quickly identify and respond to ongoing security breaches.
- Contain the security breach and stop the loss of sensitive data.
- Preemptively prevent attacks by securing all exploitable avenues.
- Apply lessons learned to further strengthen defenses and prevent repeat incidents.

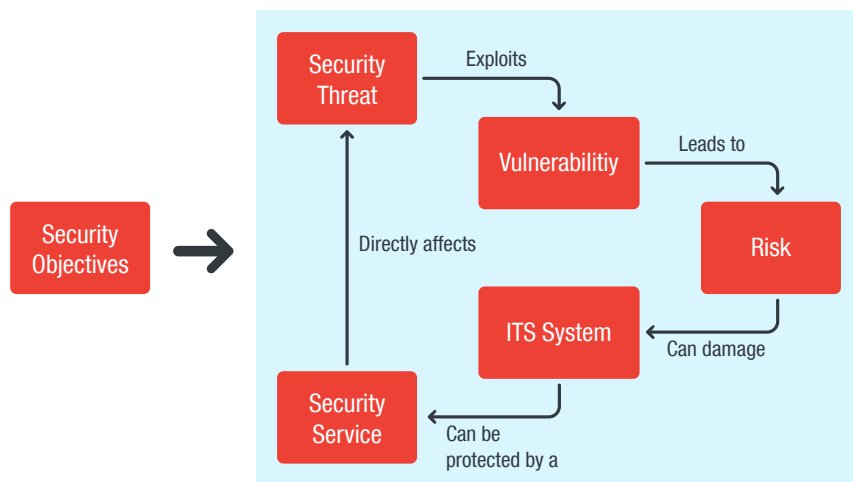


Figure 28. ITS security defense map

(Source: U.S. National ITS Architecture Security report³⁶)

Technology Discussion for IT Security Professionals

Based on our research findings on the different types of cyberthreats faced by ITS, our recommendations for the implementation of defensive strategies that we consider a mandatory minimum for ITS operators are as follows³⁷:

- **Network segmentation** — This refers to splitting a network into multiple subnetworks to reduce congestion, limit failures, and improve security. Putting all the ITS controllers on a dedicated network, that is separate from the corporate network, reduces risks of lateral movement and improves overall security.
- **Firewalls** — Network security systems that control incoming and outgoing traffic based on an applied rule set. Firewalls monitor both ingress and egress traffic from unknown and bad domains and identifies applications or endpoints that generate or request bad traffic.
- **Next-generation firewalls/Unified Threat Management (UTM) gateways** — Network security products that unify multiple systems and services into a single engine or appliance. They can incorporate firewalls, Intrusion Prevention System/Intrusion Detection System (IPS/IDS), anti-virus, web filtering, application control, and other solutions all in the same appliance. These devices analyze network traffic at line speed, and generally have lower traffic throughput compared to next-generation firewalls.
- **Anti-malware** — Software that scans files to detect, block, and remove malware such as viruses, Trojans, worms, keyloggers, ransomware, rootkits, and so on, from the system. Anti-malware uses heuristics, generic, and specific signatures to detect known and unknown malware.

- **Anti-phishing solutions** — Email-filtering products that scan for and block incoming spam and phishing emails. Spear-phishing is one of the top infection vectors. Some anti-phishing solutions also use message sandboxes to screen for potentially malicious attachments.
- **Breach Detection Systems (BDS)** — Security solutions focused on detecting intrusions caused by targeted attacks and other sophisticated threats designed to harvest information from the compromised systems. BDS analyzes complex attacks out-of-band, detecting rather than preventing network breaches. They can also analyze network traffic patterns across multiple protocols, identify malicious domains, and use emulation-sandboxing to model the behavior and impact of malicious files that are being dropped or downloaded.
- **IPS/IDS** — Network security systems that examine traffic flow to detect and prevent network attacks. IDS are passive systems that generate a report when a known bad event is identified. IPS rejects the packet when a known bad event is identified. IPS/IDS monitor the entire network for suspicious traffic by analyzing protocols and doing deep packet inspection.
- **Encryption technologies** — Software for the encryption and decryption of data in the form of files, email messages, or packets sent over a network. Encrypted network traffic will defeat Man-in-the-Middle (MitM) network-sniffing data theft attacks.
- **Patch management (physical or virtual)** — Patch management software keeps endpoints, servers, and remote computers updated by applying the latest security patches and software updates. Virtual patch management uses a security enforcement layer to prevent malicious traffic from reaching vulnerable systems. In a large IT environment where patches need to be thoroughly tested before applying it to all nodes in the network, virtual patching provides the stopgap measure of filtering out malicious traffic attempting to exploit known vulnerabilities.
- **Vulnerability scanner** — An automated tool that scans endpoints, servers, networks, and applications for security vulnerabilities that an attacker can exploit. One of the tried-and-tested ways malware does lateral movement is by exploiting vulnerabilities on the target machine it wants to infect. A vulnerability scanner scans and identifies unpatched vulnerable endpoints, servers, and applications, which the IT administrator can then patch.
- **Shodan scanning** — Shodan is a search engine for internet-connected devices. Shodan provides an easy one-stop solution to conduct Open-Source INTelligence (OSINT) gathering for different geographic locations, organizations, devices, services, etc. Software and firmware information collected by Shodan can potentially help identify unpatched vulnerabilities in the exposed cyber assets. ITS operators should monitor their IP ranges in Shodan to ensure their managed devices and systems are not exposed on the internet.

Policy Recommendations for Decision-Makers

An ITS ecosystem is essentially a massive Industrial Internet of Things (IIoT) operating environment. Policy and legislation governing operations, technology, interactions, safety and security, etc., are being actively crafted by decisions-makers at all levels of government in partnership with the ITS industry. As part of our discussion on ITS cybersecurity, we wanted to touch on some policy recommendations that we consider are crucial to the safe and reliable operations of ITS:

- Countries are actively working on defining and creating their own ITS frameworks to meet their unique future transportation needs. Countries that share land borders and have extensive transportation links (e.g., roads, rail, water) should coordinate with each other to form working groups to define a common, secure, and interoperable ITS framework. This way, the bordering countries are not left tasked with trying to integrate each other's incompatible ITS frameworks. The European ITS Framework Architecture is a good example of how these frameworks should be developed.
- A mandate in ITS framework development must be to include cybersecurity requirements to protect the ITS ecosystem. In today's connected world of smart devices and ever-increasing volumes of disruptive and destructive cyberattacks, ITS cybersecurity is mandatory.



Figure 29. Security in the U.S. National ITS Architecture

(Source: US National ITS Architecture Security report³⁴)

- One of the key operational requirements for ITS is Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I) communications. As such, standardized secure communications protocols need to be defined for ITS. Upgrading existing communications protocol families will be more cost effective than developing brand new communications protocols. Also, multiple protocols are required in ITS to handle: low bandwidth, high bandwidth, short range, long range, broadcast, multicast, one-to-one, and other communications.

- The ITS ecosystem will generate massive amounts of daily user data. This data needs to be securely stored, and strict data access usage policies need to be defined and enforced to protect the privacy and rights of all roadway users.
- Legislation should be drafted to define the permissible operational boundaries of autonomous vehicles. These operational boundaries should include policies for liability implications, accident protocols, permissible ethical actions for autonomous vehicles, data collection and recording, communications, interactions with other roadway users, etc.
- Legislation that codifies the minimum security standards (both cyber and physical) that new ITS installations, constructions, and road vehicles must satisfy before roadworthy approval is granted should be drafted. In addition, a certifying group and certification process must also be made and then organized.

Conclusion

Many of today's road networks are quickly getting congested because of the current global trends in industrialization and urbanization. These road networks are limited by plans made during another era when the population size was smaller, and urban planners failed to anticipate today's population boom. In the more densely populated cities, there is very little actual physical space available to add extra capacity to the existing road networks. Instead of building new roads, ITS technology allows municipalities to significantly increase the utilization of existing roads at a fraction of the cost of building new road infrastructure.

On the other hand, existing road infrastructure is aging and reaching their end-of-life. Municipalities have to replace these aging roads because they are no longer deemed safe for daily use. Instead of building more of the same, governments are now opting to build smart roads to future-proof themselves. There is a twofold push for the global rollout and integration of ITS, and this development trend is expected to continue over the next few decades.

A 2015 discussion paper written by David Ticoll from the University of Toronto's Munk School of Global Affairs³⁸ summarizes consultants' and analysts' predictions for autonomous vehicle (AV) adoption:

2015	Morgan Stanley: Limited driver substitution begins to roll out
2018	Morgan Stanley: Complete autonomous capability begins to roll out
2020	PwC: Semi- and full-AVs have 9-10% global share in basic scenario; 12-13% in disruptive scenario
2025	PwC: Semi- and full-AVs have 14-16% global share in basic scenario; 19-22% in disruptive scenario Goldman Sachs: Full AVs will be "commonplace"
2028	McKinsey: Consumers begin to adopt AVs
2030	PwC: Semi- and full-AVs have 15-18% global share in basic scenario; 28-30% in disruptive scenario Gartner: AVs are 25% of passenger vehicle population in use in mature markets
2035	Morgan Stanley: 100% autonomous penetration
2040-2050	McKinsey: AVs become the primary means of transport

ITS, today, is still in an “early development phase” where we are envisioning solutions, building proof of concepts, testing boundaries, defining parameters, defining tolerances, identifying threats, capacity planning, creating legislation, etc. If the predictions hold true, then we can expect a massive transportation revolution over the coming three decades. Adoption of AV will fuel big investments in ITS infrastructure, as smart roads will be needed for everyday AV operations.

In today’s connected world of smart devices and ever-increasing volumes of disruptive and destructive cyberattacks, ITS cybersecurity is mandatory and should be considered a fundamental pillar in ITS architectures and frameworks. By identifying and addressing the cybersecurity risks faced by ITS in the early development stages, we have the opportunity to influence both legislative and technological developments in ITS, which is the goal of this research paper.

Appendix

Connected Vehicle Technologies

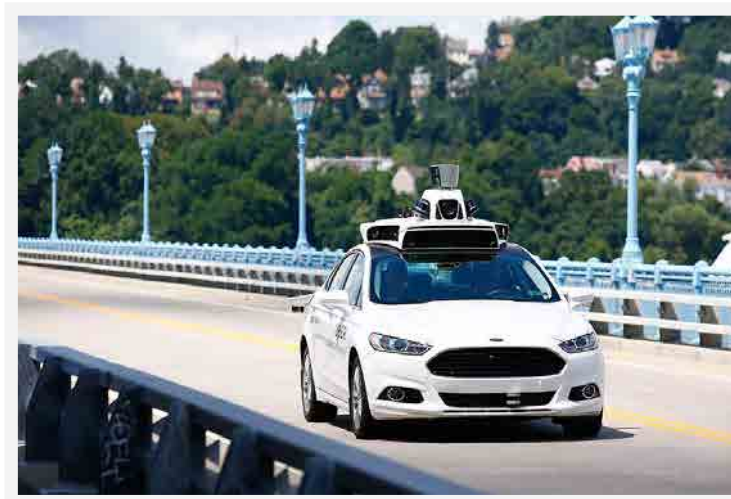


(Source: <https://www.lairdtech.com/news/laird-featured-industry-leader-connected-vehicles>)

- **GPS** — The Global Positioning System (GPS) is a space-based radio navigation system. The global navigation satellite network provides geolocation and time information to a GPS receiver on earth. Connected vehicles use GPS to pinpoint their exact location within 2 meters accuracy.
- **RADAR** — Radio Detection and Ranging (RADAR) originated from military technology. The Millimeter Wave Radar (MMW) is a dual frequency (Ka- and W-Band) mono-pulse tracking radar. MMW radar is installed under the front bumper of the car. It is the underlying sensor for many functions, e.g., front collision avoidance and traffic-aware Adaptive Cruise Control (ACC).
- **Ultrasonic sensors** — This system monitors the front and rear of the vehicle and warns the driver if there are obstacles in the vicinity of the vehicle that can cause a collision. Ultrasonic sensors are also used in functions like semi- or fully automatic parking and parking space detection. The steering functions of the vehicle during semi- or fully automatic parking are controlled by readings from the ultrasonic sensors.
- **Stereovision cameras** — On-board cameras, mounted on the windshield, handles visual recognition of the vehicle's surroundings during semi- or fully autonomous driving. Visual recognition elements include lanes, traffic signs, traffic lights, other vehicles, pedestrians, etc.
- **Lane Keep Assist (LKA)** — A system of cameras that can detect, under certain conditions, if the vehicle is veering off the lane. The LKA will automatically adjust the steering wheel to correct the vehicle's course and keep the vehicle inside the lane.

- **Telematics and OTA services** — Telematics services provide the driver with information about the route, traffic congestion, road obstacles, accident alerts, roadside assistance, and eCall. Over-the-air (OTA) programming is used for distributing new software updates, update configuration settings, and even update encryption keys for the telematics system. Telematics and OTA services are implemented using GPRS, 3G, or 4G/LTE.

Autonomous Vehicle Technologies



(Source: <https://www.americanprogress.org/issues/green/reports/2016/11/18/292588/the-impact-of-vehicle-automation-on-carbon-emissions-where-uncertainty-lies/>)

- **LIDAR** — A portmanteau of “light” and “radar,” it is a type of range-finding sensor that emits laser pulses and measures the time it takes the pulses to reflect off a distant surface. The laser pulses are bounced off of a spinning mirror rotating thousands of times per second, thus creating a scan of laser pulses. The echoes are used to detect objects on the road under any weather condition. LIDAR is commonly used for ACC and collision avoidance.
- **Infrared headlamps** — These extend vision at night without blinding other drivers. The signature of the infrared beams is detected by an infrared camera, which does visual recognition analysis for pedestrians and other objects on the road.
- **V2V and V2I communications** — In the future, autonomous vehicles will be mandated to communicate, in an ad-hoc manner, with other connected vehicles and smart road infrastructure, providing them information such as location data, safety warnings (e.g., when driving through an intersection), and surrounding traffic information. Communications will be done using wireless technology such as 3G, 4G/LTE, 802.11g/n/p, 802.16, etc. The wireless communications standard and messaging format is still to be determined.

Roadway Reporting Technologies



(Source: <http://www.bbc.com/news/uk-scotland-highlands-islands-30972743>)

- **Bus lane cameras** — Most mid-to-large sized cities have a system of bus lanes that gives priority to transit vehicles during peak traffic hours. The city enforces the bus lanes using cameras that take photos/videos of violators and issues them fines.
- **High Occupancy Vehicle (HOV) lane cameras** — HOV lanes are reserved for vehicles with two or more occupants during peak traffic hours. There are also permanently designated HOV lanes in freeways. The city enforces HOV lanes using a camera network that takes photos/videos of violators and issues them fines.
- **Red light cameras** — Are placed at traffic intersections to reduce the number of crashes. These cameras take photos/videos of vehicles that deliberately violate a red light and the city issues them fines.
- **Speed cameras** — Are used to monitor if vehicles are complying with posted speed limits. The system has a built-in radar that can measure vehicle speed. The speed cameras take photos/videos of violators and the city issues them fines.
- **Railway crossing cameras** — Cameras that monitor traffic at railway crossings. These cameras operate like red light and speed cameras combined. When the camera detects an incident, the vehicle information is sent to the control center for verification. The control center may issue the offending vehicle a fine or take other actions.
- **Automatic Number Plate Recognition (ANPR)** — ANPR technology is used in traffic cameras that are used for issuing automatic fines, parking enforcement, toll collection, border crossings, etc.
- **Induction loop** — Is an electromagnetic vehicle detection system that generates an electric current when a vehicle stops over it. Induction loops are commonly found placed at intersections to send control signals to the traffic lights.

- **Vehicle detection systems** — Have extensive capabilities, accuracy, and versatility of different types, such as: speed, vehicle counts, vehicle classifications, stopped vehicle detection, wrong way vehicles, accident detection, as well as other traffic data, e.g., occupancy, gap between vehicles, queue detection, etc.³⁹ This data is used by the central control for traffic flow monitoring.
- **UAV road monitoring** — Unmanned Aerial Vehicles (UAVs) are increasingly being used in civilian applications. In the future, traffic control centers will use UAVs to monitor traffic and enforce rules in remote roadway locations.
- **Roadside weather stations** — Measures environmental variables such as road surface temperature, water film thickness, barometric pressure, temperature, etc. This provides precise information about the current road conditions that is then used by central control to make safety decisions.
- **Emissions/Air quality sensors** — Are used to measure air quality at the roadway level. It is very important to monitor air quality from a health and safety perspective, especially in cities with heavy traffic, overpopulation, large manufacturing base, lots of commercial vehicle traffic, etc.
- **Vehicle location tracking (via GPS, V2I, sight, etc.)** — Future ITS infrastructure will support both V2V and V2I communications that will report the vehicle location to improve road safety. Currently, vehicle tracking can be done via ANPR cameras. Commercial vehicles have GPS trackers that report vehicle location to the company fleet control centers.

Traffic Flow Control Technologies



(Source: https://en.wikipedia.org/wiki/Variable-message_sign)

- **Reversible lanes** — Are lanes in which traffic may travel in either direction, depending on the displayed overhead signal (a green arrow or a red cross). Reversible lanes are used to improve traffic flow during rush hour.⁴⁰
- **Railway crossing barriers** — Physical barriers that are lowered in front of road-railway crossings to prevent vehicle movement when a train is approaching. These barriers are controlled by the railway track's switch control.
- **Dynamic message signs** — Are above roadway gantry mounted electronic traffic signs for displaying important messages to travelers. These signs are used for displaying messages about traffic congestion, accidents or incidents, road works, speed limits, wait times, lane signals, etc.
- **Dynamic road surface markers** — These are in-pavement LED markers that are used for dynamically delineating lane markings. They can be used to invoke contraflow lanes, mark pedestrian crossings, mark shoulders, add lanes, or improve lane visibility in bad weather.
- **Dynamic road barriers** — Work in conjunction with reversible lane signals, railway switch controls, toll collection systems, etc., to lower or raise physical gates that change the traffic flow.
- **Traffic signal control systems** — Are placed at intersections to coordinate and control the intersection's traffic lights. Traffic lights are operated via control signals sent from road-embedded induction loops or roadside sensors and detectors; via signals sent from the central control over a public IP network or over VPN; or at preset time intervals.
- **Ramp meter** — Is a basic traffic light (red and green only) together with a signal controller that regulates the flow of traffic entering freeways according to current traffic conditions.⁴¹ The regulated ingress of cars into the freeway using ramp meters reduces excessive congestion.
- **Pedestrian detectors** — Installed at intersections and crosswalks, uses a combination of cameras and sensors to detect pedestrians. The pedestrian detection system controls traffic lights or pedestrian warning lights, e.g., flashing beacons.
- **Bicyclist detectors** — Are similar to pedestrian detectors. The detector uses a combination of cameras and sensors, such as infrared, to identify bicyclists and sends control signals to the traffic light control system.
- **Automated toll collection systems** — These are dynamic gates that allow vehicles to pass after paying toll. They control traffic flow on tolled roadways. (This excludes automatic toll collection systems that use ANPR to bill vehicles and have no gate controls.)
- **Emergency vehicle priority system** — Allows emergency vehicles, e.g., fire trucks, ambulances, and police vehicles, to automatically trigger traffic light sequences along the most direct route when responding to an emergency. By clearing the path ahead, emergency vehicles can respond more quickly.⁴²

- **Transit signal priority (TSP)** — Is a set of operational improvements that reduce wait time at traffic signals for transit vehicles by holding green lights longer or shortening red lights. TSP may be implemented at individual intersections, across corridors, or entire street systems.⁴³
- **Safety systems for autonomous vehicles** — This is a two-way V2I communication network setup along the roadway to provide autonomous vehicles with road, traffic, location, and other important information. The autonomous vehicles can change speed, in-between vehicle gaps, and travel routes based on the information received.
- **Dedicated lanes for autonomous vehicles** — For autonomous vehicles to become a reality, in the first stage of introduction there will be dedicated travel lanes for autonomous vehicles. These lanes will be enforced using dynamic message signs, dynamic road surface markers, ramp meters, and gate controls.

Payment Applications and Systems Technologies



(Source: https://en.wikipedia.org/wiki/Electronic_toll_collection)

- **Radio Frequency Identification (RFID) payments** — RFID chips are embedded in smart payment cards and vehicle sticker tags. These RFID chips are used for identifying and billing the vehicles.
- **Kiosk payments** — These are ticket vending machines commonly found at stations. They accept NFC, RFID, credit/debit card, and cash payments. New tickets can be purchased, old ones extended, smart card balances reloaded, etc.
- **Ticket payments** — Transit payment systems support physical tickets. Tickets issued at kiosks will either have a magnetic stripe or embedded RFID chip that validates the ticket. Tickets purchased online and then printed out have a Quick Response (QR) code or barcode for validation scanning.
- **App payments** — Smart phone apps allow users to purchase e-tickets. The user validates the e-ticket by scanning the displayed barcode or QR code at the entry gate.

- **ANPR automatic payments** — Runs algorithms to read the vehicle's license plate under any light and weather condition. If there is a billable account setup for the license plate, then that account is charged; else, a physical bill is mailed to the customer with instructions on how to pay.
- **Dynamic tolling** — Tolled roadways charge different rates based on the time of the day, i.e., higher rate during peak hours and cheaper rate during off-peak hours. Tollbooths are being replaced with ANPR payments and RFID vehicle sticker tags.
- **Congestion zone charges** — In cities with high population densities, e.g., London, municipalities have introduced congestion zone charges in the city center to discourage people from driving into the city and instead encourage them to use public transportation. Drivers can purchase congestion zone vehicle passes, or vehicles are billed using ANPR automatic payments.
- **Parkade payments** — There are multiple ways of paying for parking at a parkade: payment via kiosk, payment on exit at the cashier, paying via RFID vehicle sticker tag (for parking pass holders), ANPR automatic payments, smart phone app, etc.
- **Roadside parking payments** — Payments using coins is now being replaced with payments via phone, via smart phone app, or using built-in credit card payment processing machines.
- **Freight truck tolls** — Truck-weighing stations are located on highways/freeways; commercial trucks are required by law to get weighed. This generates revenue for the state which maintains the highways/freeways and also ensures there are no overloaded trucks on the road.
- **Multimodal transportation payments** — In today's multimodal transit network (buses, trains, subways), transit authorities are switching to integrated single-payment systems. These are implemented using smart cards and paper tickets with embedded RFID chips.

Management Applications and Systems Technologies



(Source: <http://www.businesswire.com/news/home/20150812005074/en/City-West-Richland-Washington-Partners-Ameresco-Install>)

- **Streetlight controls** — Management system for outdoor lighting. Streetlights are normally controlled by ambient light sensors or timers, but the ITS control center can monitor and control streetlights individually or in groups. A streetlight management system helps conserve energy, reduces costs, simplifies maintenance, and allows for centralized monitoring.
- **Disaster management** — These are a set of procedures activated by the ITS control centers when disaster strikes a municipality. Disasters could be natural calamities, freak accidents, terrorist attacks, etc. Disaster management will typically include opening evacuation routes, plans for first responders, public communications plans, and such.
- **Information sharing services** — The ITS ecosystem generates massive amounts of data daily. This data is used across multiple departments for traffic management, for billings, for planning and policy decisions, for creating maintenance schedules, etc. ITS control centers, which are the data collection points, have data sharing services setup for secure and easy access to the data.
- **Data management and storage systems** — To process and store big data the ITS ecosystem generates, the control center needs to maintain large data centers. ITS data must be protected and access controlled, so as not to breach user's privacy rights; for example, no one should be able to track a person's vehicle movements without legal authorization.
- **Smart parking management** — Remote-sensing devices in parkades monitor available spaces and share that information with connected cars, mobile apps, and dynamic signage. Parkades in the near future will coordinate available parking spaces to maximize utilization and revenue.

- **Billing and toll administration** — All types of daily transactions, e.g., parkade payments, dynamic tolling, congestion zone charges, ANPR payments, ticket payments, etc., need to be processed quickly and accurately. Billing systems can directly impact traffic flow control mechanisms such as entry gates at tolled bridges and highways.
- **Transit vehicle management** — Tracks the real-time position of transit vehicles and uses that information to update/create route schedules and maintenance schedules, identify operational deficiencies, etc. The real-time position and expected arrival time information are made available at bus stops, on the web, on transit apps, and such.
- **Emergency vehicle management** — System used by dispatchers to track, route, and quickly send help to the location of the emergency. The system will give traffic signal priority to emergency vehicles at intersections so they can safely reach their destination in the shortest possible time.
- **Traffic and congestion management** — These systems control reversible lanes, dynamic road surface markers, dynamic message signs, intersection traffic lights, and such. These are the most important systems in the ITS ecosystem because they are used for managing/controlling the traffic flow of the entire roadway network.
- **Smart traffic light control systems** — Are a subsystem of traffic and congestion management. Traffic lights communicate with the ITS control center over a public IP network or over VPN. The control center can change the traffic signal behavior to give priority to emergency and traffic vehicles, or change the traffic signal behavior altogether as the situation demands.
- **Commercial vehicle operations** — These are systems run by freight companies to keep track of their fleet. The system tracks vehicle locations, does delivery scheduling and routing in the most efficient manner, processes all required clearance paperwork including for border crossings, manages payment of toll and other surcharges, etc. The system is designed to improve operational efficiency, reduce costs, and increase revenue. When autonomous trucks start driving on the road, these systems will be used to coordinate road trains for super density operations.
- **Maintenance and construction management** — Roadways and their supporting infrastructure are in need of regular maintenance, and new roadway constructions are always in the planning pipeline. Engineering depends on ITS data to plan and schedule repairs and identify new construction opportunities.
- **Cooperative traffic and position sharing systems** — In the future, connected cars and autonomous vehicles will be ad-hoc sharing their location with each other and with road infrastructure. The ITS ecosystem will need to process received vehicle location data in real-time and share it with the rest of the roadway network and the other nearby connected vehicles. This location data will be used for safety improvement and for traffic flow control.

- **Artificial intelligence (AI) and machine learning (ML) applications** — AI and ML applications aim to extract value from big data. For ITS, the goal for AI and ML will be to improve system efficiency, traffic flow prediction models, and disaster response modeling, identify future construction opportunities, create new revenue generation models, improve city expansion modeling, reduce cost, etc. This data analysis is crucial to both city planners and government decision-makers.
- **Road-based location services for autonomous vehicles** — To improve the location accuracy of autonomous vehicles, the ITS ecosystem will have land-based GPS transmitters. These transmitters will transmit their exact location as well as other data including traffic, accident/incident information, weather, etc.

Communication Applications and Systems Technologies



(Source: <http://carsonsigns.com.au/>)

- **Smart apps** — The global median for smartphone ownership is 43% and in developed countries, that number increases to more than 50%.⁴⁴ ITS apps, running on smartphones, are making it easier for users to pay for and use various ITS services. Apps are currently being used for: transit, e-tickets, traffic, car sharing, freight hailing, taxi/limo hailing, parking, trip planning, ride sharing, vehicle diagnostics and management, etc.
- **Social media** — A growing size of the population receives their daily news from social media platforms like Twitter and Facebook. ITS operators routinely update the public with important information such as transit delays, strikes, etc., through social media platforms.

- **Company website** — In conjunction with social media, company websites also host important user information for ITS services. Additionally, the websites provide services like trip planning, ticket purchase, fare payments, schedules, etc.
- **Advertisements** — Are one of the major revenue streams for ITS providers. Digital advertisements on display screens are slowly supplanting the traditional print and poster advertisements, although print and posters are not expected to disappear completely anytime soon.
- **Passenger travel information** — The real-time locations of transit vehicles and their expected arrival/departure times are made available to users via: digital message boards at transit stops, smartphone apps, SMS, and on the company website.
- **Road obstacle and accident alerts** — Will be displayed on the dynamic message signs above highways/freeways. They are broadcast to vehicles which have Traffic Message Channel (TMC) enabled. In the future, obstacle and accident alerts will be broadcast via V2V and V2I channels.
- **Telematics and eCall** — Telematics services provide the driver with information about the route, traffic congestion, road obstacles, accident alerts, roadside assistance, and eCall. eCall can connect the vehicle to roadside assistance or with emergency services. eCalls to emergency services can be done manually or automatically if the vehicle detects it is in an accident.
- **Emergency vehicle warning systems** — In the future, emergency vehicles will be able to send a voice warning to the FM radio receiver of the car in front advising them to move aside.⁴⁵ Additionally, V2V/V2I messages will audibly and visibly warn drivers to move aside for emergency vehicles.
- **Road information displays and alert systems** — Are above roadway gantry mounted electronic traffic signs for displaying important messages to travelers. These signs are used for displaying messages about traffic congestion, accidents or incidents, road works, speed limits, wait times, lane signals, etc.
- **Communication cell towers, antennas, and repeaters** — These are the backbone hardware for ITS communications. There is a shared responsibility between the telco and ITS providers for the installation, upkeep, and maintenance of the communication hardware.
- **I2I, V2V, and V2I communications** — In the future, all connected vehicles will be mandated to communicate, in an ad-hoc manner, with other connected vehicles and smart road infrastructure, providing them information such as: location data, safety warnings, and surrounding traffic information. Communications will be done using wireless technology such as: 3G, 4G/LTE, 5G, 802.11g/n/p, 802.16, etc.

References

1. Intelligent Transportation Systems Society of Canada. (2012). *ITS Canada*. "Intelligent Transportation." Last accessed on 7 April 2017 at <https://www.itscanada.ca/it/>.
2. FRAME Forum. (2017). *FRAME*. "Why you need an ITS Architecture." Last accessed on 26 May 2017 at <http://frame-online.eu/first-view/why-you-need-an-its-architecture>.
3. Tom Steele. (23 May 2016). *Dallas News*. "Central Texas man says he changed highway sign to 'Drive Crazy Yall' for a laugh." Last accessed on 24 April 2017 at <https://www.dallasnews.com/news/crime/2016/05/23/central-texas-man-says-he-changed-highway-sign-to-drive-crazy-yall-for-a-laugh>.
4. Katie Mettler. (6 June 2016). *The Washington Post*. "Somebody keeps hacking these Dallas road signs with messages about Donald Trump, Bernie Sanders and Harambe the gorilla." Last accessed on 25 April 2017 at https://www.washingtonpost.com/news/morning-mix/wp/2016/06/06/somebody-keeps-hacking-these-dallas-road-signs-with-messages-about-donald-trump-bernie-sanders-and-harambe-the-gorilla/?utm_term=.d396ae2a8d66.
5. Sean Gallagher. (November 29, 2016). *Ars Technica*. "Ransomware locks up San Francisco public transportation ticket machines." Last accessed: October 17, 2017. <https://arstechnica.com/information-technology/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/>.
6. Stephen Hilt and Fernando Mercês. (November 30, 2016). *TrendLabs Security Intelligence Blog*. "HDDCryptor: Subtle Updates, Still a Credible Threat." Last accessed: October 17, 2017. <http://blog.trendmicro.com/trendlabs-security-intelligence/hddcryptor-updates-still-credible-threat/>.
7. Joe Fitzgerald Rodriguez. (26 November 2016). *San Francisco Examiner*. "'You Hacked' appears at Muni stations as fare payment system crashes." Last accessed on 25 April 2017 at <http://www.sfexaminer.com/hacked-appears-muni-stations-fare-payment-system-crashes/>.
8. Clarence Williams. (27 January 2017). *The Washington Post*. "Hackers hit D.C. police closed-circuit camera network, city officials disclose." Last accessed on 25 April 2017. https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.39a287b8b971.
9. Samira Said. (9 April 2017). *CNN*. "Hacker sets off emergency alarms, frightening Dallas residents." Last accessed on 25 April 2017. <http://www.cnn.com/2017/04/08/us/dallas-alarm-hack/index.html>.
10. Lily Hay Newman. (10 April 2017). *Wired*. "That Dallas Siren Hack Wasn't Novel – It Was Just Really Loud." Last accessed on 25 April 2017. <https://www.wired.com/2017/04/dallas-siren-hack-wasnt-novel-just-really-loud/>.
11. Alessa Brings and Stefani Geilhausen. (21 April 2017). *RP Online*. "Wie Hightech am Donnerstag die Rheinbahn lahm legte." Last accessed on 28 April 2017. <http://www.rp-online.de/nrw/staedte/duesseldorf/wie-hightech-am-donnerstag-die-rheinbahn-lahm-legte-aid-1.6768928>.
12. Radio Liberty. (13 May 2017). *Radio Liberty*. "Компьютеры РЖД подверглись хакерской атаке и заражены вирусом." Last accessed on 14 May 2017 at <https://www.svoboda.org/a/28483898.html>.
13. BBC. (May 14, 2017). *BBC News*. "Ransomware cyber-attack threat escalating - Europol." Last accessed on 14 May 2017 at <http://www.bbc.co.uk/news/technology-39913630>.
14. Chris Graham. (13 May 2017). *The Telegraph*. "Cyber attack hits German train stations as hackers target Deutsche Bahn." Last accessed on 14 May 2017 at <http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/>.
15. Trend Micro, Inc. (12 May 2017). *TrendLabs Security Intelligence Blog*. "Massive WannaCry/Wcry Ransomware Attack Hits Various Countries." Last accessed on 30 August 2017 at <http://blog.trendmicro.com/trendlabs-security-intelligence/massive->

wannacrywcry-ransomware-attack-hits-various-countries.

16. Pete Muntean. (17 May 2017). *USA Today*. "Porn plays on screen in D.C.'s Union Station." Last accessed on at 23 May 2017 at <https://www.usatoday.com/story/news/nation-now/2017/05/17/porn-plays-screens-d-c-s-union-station/327411001/>.
17. Kim Zetter. (26 July 2017). *Vice Motherboard*. "Car Wash Hack Can Strike Vehicle, Trap Passengers, Douse Them With Water." Last accessed on 10 August 2017 at https://motherboard.vice.com/en_us/article/bjxe33/car-wash-hack-can-smash-vehicle-trap-passengers-douse-them-with-water.
18. John Beltz Snyder. (4 August 2017). *Autoblog*. "Researchers hack a self-driving car by putting stickers on street signs." Last accessed on 10 August 2017 at <https://www.autoblog.com/2017/08/04/self-driving-car-sign-hack-stickers/>.
19. Jessica Morgan. (4 August 2017). *Evening Standard*. "California road sign hacked to read 'Trump Has Herpes'." Last accessed on 10 August 2017 at <https://www.standard.co.uk/news/world/california-road-sign-hacked-to-read-trump-has-herpes-a3603821.html>.
20. Carla Herreria. (7 August 2017). *HuffPost*. "California Traffic Sign Hacked To Warn People Of 'Asian Drivers'." Last accessed on 10 August 2017 at http://www.huffingtonpost.ca/entry/caution-asian-drivers-napa-traffic-sign_us_595ef341e4b0d5b458e9678e.
21. Kenneth Chan. (8 February 2017). *Daily Hive*. "Why the Canada Line's exposed tracks can't deal with snowfall." Last accessed on 6 May 2017 at <http://dailyhive.com/vancouver/canada-line-conventional-rail-linear-induction-technology-snowfall>.
22. Daniel Fund. (March 2004). *Car and Driver*. "How to Become a Felon Without Really Trying." Last accessed 24 April 2017 at <http://www.caranddriver.com/columns/how-to-become-a-felon-without-really-trying>.
23. NBC New York. (2016). *NBC New York News*. "Timeline: New Jersey's George Washington Bridge Scandal." Last accessed on 24 April 2017 at <http://www.nbcnewyork.com/news/local/Timeline-George-Washington-Bridge-Scandal-Chris-Christie-Fort-Lee-Bridgegate-239431091.html>.
24. Rainer Link. (28 July 2015). *TrendLabs Security Intelligence Blog*. "Is Your Car Broadcasting Too Much Information?" Last accessed on 9 May 2017 at <http://blog.trendmicro.com/trendlabs-security-intelligence/is-your-car-broadcasting-too-much-information/>.
25. Fatih Sakiz and Sevil Sen. "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV." *Ad Hoc Networks*, 61 (June 2017): 33-50. Elsevier. <http://www.sciencedirect.com/science/article/pii/S1570870517300562>.
26. Suzanne Jacobs. (19 August 2014). *MIT Technology Review*. "Researchers Hack Into Michigan's Traffic Lights." Last accessed on 10 August 2017 at <https://www.technologyreview.com/s/530216/researchers-hack-into-michigans-traffic-lights/>.
27. Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman (2014). Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT '14). Last accessed on 2 May 2017. <https://jhalderm.com/pub/papers/traffic-woot14.pdf>.
28. Lucian Constantin. (18 December 2014). *CIO*. "Vulnerability in embedded Web server exposes millions of routers to hacking." Last accessed on 26 May 2017 at <http://www.cio.com/article/2861233/vulnerability-in-embedded-web-server-exposes-millions-of-routers-to-hacking.html>.
29. Joey Costoya, Ryan Flores, Lion Gu, and Fernando Mercês. (29 December 2016). *Trend Micro*. "Securing Your Home Router – Understanding Attacks and Defense Strategies." Last accessed on 26 May 2017 at <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-securing-your-home-routers.pdf>.
30. Numaan Huq, Stephen Hilt, and Natasha Hellberg. (15 February 2017). *Trend Micro Security News*. "US Cities Exposed in Shodan." Last accessed on 26 May 2017 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/us-cities-exposed-in-shodan>.

31. Murugiah Souppaya and Karen Scarfone. (March 2016). *U.S. Department of Commerce*. Draft NIST Special Publication 800-154, "Guide to Data-Centric System Threat Modeling." Last accessed on 30 August 2017 at http://csrc.nist.gov/publications/drafts/800-154/sp800_154_draft.pdf.
32. Microsoft. (June 2003). *Microsoft Developer Network*. "Chapter 3 Threat Modeling." Last accessed on 14 May 2017 at <https://msdn.microsoft.com/en-us/library/aa302419.aspx>.
33. David Czagan. (21 May 2014). *InfoSec Institute*. "Qualitative Risk Analysis with the DREAD Model." Last accessed on 14 May 2017 at <http://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model/>.
34. Ibid.
35. Microsoft. (June 2003). Op. cit.
36. U.S. Department of Transportation Architecture Development Team. (October 2003). "National ITS Architecture Security." Last accessed on 16 May 2017 at <https://www.hSDL.org/?view&did=484293>.
37. Numaan Huq. (11 March 2015). *Trend Micro*. "Defending Against PoS RAM Scrapers: Current and Next-Generation Technologies." Last accessed on 16 May 2017 at <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-defending-against-pos-ram-scrapers.pdf>.
38. David Ticoll. (15 October 2015). *University of Toronto Munk School of Global Affairs*. "Driving Changes: Automated Vehicles in Toronto." Last accessed on 16 May 2017 at [https://www1.toronto.ca/City%20Of%20Toronto/Transportation%20Services/TS%20Publications/Reports/Driving%20Changes%20\(Ticoll%202015\).pdf](https://www1.toronto.ca/City%20Of%20Toronto/Transportation%20Services/TS%20Publications/Reports/Driving%20Changes%20(Ticoll%202015).pdf).
39. Axiomtek. (2017). *Axiomtek*. "Vehicle Detection System." Last accessed on 16 April 2017 at <http://www.axiomtek.com/Default.aspx?MenuId=Solutions&FunctionId=SolutionView&ItemId=36&Title=Vehicle+Detection+System>.
40. Drivesed.com. (2017). *Edriving*. "Reversible Lanes." Last accessed on 17 April 2017. https://drivesed.com/resources/terms/reversible_lanes.aspx.
41. Wikimedia. (8 March 2017). *Wikipedia*. "Ramp meter." Last accessed on 17 April 2017 at https://en.wikipedia.org/wiki/Ramp_meter.
42. Queensland Government. (24 February 2017). *Department of Transport and Main Roads*. "Emergency Vehicle Priority." Last accessed on 17 April 2017 at <http://www.tmr.qld.gov.au/Safety/Road-safety/Emergency-Vehicle-Priority.aspx>.
43. TransitWiki. (31 October 2016). *TransitWiki*. "Transit signal priority (TSP)." Last accessed on 17 April 2017 at [https://www.transitwiki.org/TransitWiki/index.php/Transit_signal_priority_\(TSP\)](https://www.transitwiki.org/TransitWiki/index.php/Transit_signal_priority_(TSP)).
44. Jacob Poushter. (22 February 2016). *Pew Research Center*. "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies." Last accessed on 20 April 2017 at <http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/>.
45. Jayesh Shinde. (18 January 2017). *India Times*. "Swedish Ambulances Will Hack Into Car Audio Remotely To Ask People To Get Out Of The Way." Last accessed on 21 April 2017 at <http://www.indiatimes.com/technology/news/swedish-ambulances-refuse-to-get-stuck-in-traffic-to-mute-car-audio-remotely-to-alert-drivers-269782.html>.



Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud

www.trendmicro.com