INL/CON-15-35332
PREPRINT

Impacts of Vehicle (In)Security

IAEA International Conference on Computer Security in a Nuclear World

J. Chugg and K. Rohde

May 2015

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Impacts of Vehicle (In)Security

J. Chugg[1], K. Rohde[1]

[1]Idaho National Laboratory, Idaho Falls, Idaho, USA

E-mail contact of main author: jonathan.chugg@inl.gov

Abstract. Nuclear and radioactive material is routinely transported worldwide every day. Since 2010, the complexity of the transport vehicle to support such activities has grown exponentially. Many core functions of a vehicle (e.g., braking, steering, traction control, etc.) are now handled by small embedded computer modules and more modules are being added each year to enhance the owner's experience and convenience (e.g., infotainment, navigation, communications, etc.). With a system as complex as today's automobile, the potential for cyber security issues is certain. The hacker community has begun exploring this new domain and public information is increasingly disseminated. Because vehicles are allowed into and around secure nuclear facilities, the potential for using a vehicle as a new cyber entry point or vector into the facility is now plausible and must be mitigated. In addition, compromising such a vehicle could aide in illicit removal of nuclear material, putting sensitive cargo at risk. Because cyber attacks can now be introduced using vehicles, cyber security, needs to be integrated into an organization's design basis threat document. Essentially, a vehicle now extends the perimeter for which security professionals are responsible.

Electronic Control Units (ECU) responsible for handling all core and ancillary vehicle functions are interconnected using the controller area network (CAN) bus. The CAN protocol was developed during the early 1980s and first released in 1987 on a handful of devices for use in passenger cars. A typical CAN network in a modern automobile contains 50 or more ECUs. The CAN protocol has grown and now supports many different protocols that are used in a wide variety of areas, including automotive, road transportation, rail transportation, industrial automation, power generation, maritime, military vehicles, aviation, and medical devices. In more than one way, the nuclear industry is employing the CAN bus protocol or other similar broadcast serial networks. This paper will provide an overview of the current state of automobile and CAN Bus security, as well as an overview of what has been publicly disclosed by many research organizations. It will then present several hypotheses of how vehicle security issues may impact nuclear activities. An initial discussion of how a vehicle can be used as a new threat vector to penetrate secure facilities will be presented. This includes how a modern automobile can be used as the exploitation mechanism for nearby devices such as laptops, cell phones, and wireless access points. Additional discussion will highlight how vehicle security might impact transportation of nuclear material through remote exploitation of a moving vehicle. The final discussion will include what possible implications might be relative to the physical protection systems at nuclear facilities.

The audience will also be given details regarding the complexity of attack, thus implying the likelihood of successful exploitation, and information on how such attacks may be mitigated. Emerging security products for automobiles will be discussed and other mitigation methods will be detailed (e.g. disabling vehicle cellular modems). As a result, the audience will have a greater understanding of how to add vehicle security as a part of a comprehensive nuclear security policy.

Finally, this paper will highlight the similarities between CAN Bus and other broadcast serial bus networks such as Profibus or DeviceNet, helping educate the reader on how susceptible this type of networking is to nefarious attacks and how it might affect components connected to many different nuclear systems, including control systems, safety systems, emergency systems, and support systems.

Key Words: vehicle, nuclear security, CAN bus

1. Introduction

The technology used in modern vehicles has advanced very rapidly over the last 10 to 15 years. A modern automobile contains more electronics and communications networks than most people realize. This trend is true for all other vehicles found across the transportation sector; ships, freight trains, airplanes, and heavy equipment are being updated to include electronics to better manage the many sub-systems responsible for operating these transportation systems.

As electronics are added to vehicles, the complexity of these systems also increases. These new capabilities and complexity usher in a new set of potential threat vectors. The modern vehicle is much more convenient to operate (e.g., staff is reduced on a large cargo ship) and much more reliable because of these computer systems; however, the cyber security of these systems is seldom considered.

This paper will cover a wide breadth of vehicle security used in the nuclear sector. Although the discussion will be weighted toward the automobile (e.g., light trucks and passenger cars), it is directly applicable to other forms of transportation (e.g., commercial trucking, rail, maritime, etc.). The vulnerabilities discussed that might be specific to a passenger car are often times directly applicable to other vehicle systems, such as an engine management system of a large diesel generator.

The core problem with modern transportation vehicles in is their growing complexity and how that complexity is being solved by computer systems and communications networks. The computer systems and networks now used in a typical passenger car are more complex and powerful than a personal computer 15 years ago. With this new technology comes the security implications that are part of having communications with the internet.

Now that vehicle electronics are widely available to the public, the cyber security community (i.e., hackers) is now playing with these systems. Since 2013, many of the security conferences (such as Black Hat[1], DEF CON[2], and CanSecWest[3]) have included sessions that disclose and discuss security findings relative to the control systems found in automobiles. This is an exciting new area of research for the community and will continue to be relevant for many years to come. There is already news of a complete end-to-end remote vulnerability demonstration of a modern passenger car scheduled for the Black Hat conference in Las Vegas, Nevada in 2015.[4]

The Cyber Security Research and Development Department at Idaho National Laboratory[5] has supported the U.S. Department of Energy[6] and the Department of Homeland Security[7]

---

[1] Black Hat USA, https://www.blackhat.com/

[2] DEF CON, https://www.defcon.org/

[3] CanSecWest, https://cansecwest.com/

[4] *Wired Magazine*, Andy Greenberg, April 27, 2015, "Researchers Plan to Demonstrate a Wireless Car Hack this Summer," http://www.wired.com/2015/04/researchers-plan-wirelessly-hack-car-public-summer/

[5] Idaho National Laboratory, https://www.inl.gov/

[6] U.S. Department of Energy, http://energy.gov/

[7] U.S. Department of Homeland Security, http://www.dhs.gov/

with their programs to secure Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) since 2003. This work has been largely focused on systems that operate critical systems throughout critical infrastructure sectors (e.g., chemical, energy, manufacturing, and water); however, in 2013, a small research group with internal Idaho National Laboratory funding started looking into the potential security issues of a modern passenger vehicle.

2. Vehicle Control Systems Overview

Complex systems, such as an automobile, have always required some level of monitoring and control. For more than a century, this was accomplished using basic analog components that required constant human interpretation and intervention. With the introduction of digital systems, many of the analog components have been replaced by more autonomous and robust microprocessing units.

Today's vehicles now contain many (i.e., sometimes hundreds) of small microprocessors, each of which is responsible for monitoring and controlling a small subsystem of a vehicle's functionality (e.g., engine control, climate control, etc.). Most of these systems are now connected to a communications bus so information can be shared and collected and commands issued and interpreted. A good example of how this evolution has transpired over the years is the basic functionality of controlling a vehicle's speed. Gone are the days of the accelerator pedal being physically connected to a cable or rod that actuates a physical valve responsible for controlling air and fuel. Today's accelerator pedal now produces a digital signal that is interpreted by a microprocessor, which then controls an actuator that is connected to a valve responsible for controlling air and fuel (drive by wire). As a result of these technological advances, many modern vehicles already have enough control to be considered Level 1 and Level 2 autonomous vehicles.[8]

Serial communication buses have been employed by digital systems for decades.[9] This simple and inexpensive form of digital communication lends itself to be employed in environments where reliable communications are required for small embedded devices and components. The serial buses most commonly found in traditional Information Technology[10] environments include RS-232[11] and RS-485[12], but ICS environments also employ specialized buses such as DeviceNet[13] or PROFIBUS.[14] All of these systems share very similar physical layers (e.g., twisted pair cables), but the protocols used to encode messages are quite different.

---

[8] U.S. Department of Transportation Automated Vehicle Development Policy, http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development

[9] Serial Communication Overview, http://en.wikipedia.org/wiki/Serial_communication

[10] Information Technology Overview, http://en.wikipedia.org/wiki/Information_technology

[11] RS-232 Overview, http://en.wikipedia.org/wiki/RS-232

[12] RS-485 Overview, http://en.wikipedia.org/wiki/RS-485

[13] DeviceNet Overview, http://en.wikipedia.org/wiki/DeviceNet

[14] PROFIBUS Overview, http://en.wikipedia.org/wiki/Profibus

One of the first communication buses developed for automotive use was the Controller Area Network (CAN) bus.[15] The CAN protocol was developed during the early 1980s and first released in 1987 on a handful of devices for use in passenger cars with the sole purpose of adding functionality. A typical CAN network in a modern automobile will contain 50 or more ECUs for a number of different subsystems, including control modules for the engine, powertrain, transmission, antilock braking, airbags, power steering, cruise control, door locks, windows, audio system, battery, and charging system. The CAN protocol has since grown and now supports many different protocols that are used in a wide variety of areas, including automotive, road transportation, rail transport, industrial automation, power generation, maritime, military vehicles, aviation, and medical devices.

Figure 1 shows an overview image of serial bus networks and components included in a typical modern vehicle. These new communication networks, along with the many ECUs required to safely operate a modern vehicle, introduce several new safety, reliability, and security vulnerabilities. These networks and devices are now communicating to the internet for many reasons (e.g., monitoring, updating, and user convenience). Most automobiles sold today have some form of remote monitoring system installed (such as OnStar[16], SYNC 3[17], and ConnectedDrive[18]), and these systems use cellular networks to allow remote connectivity.

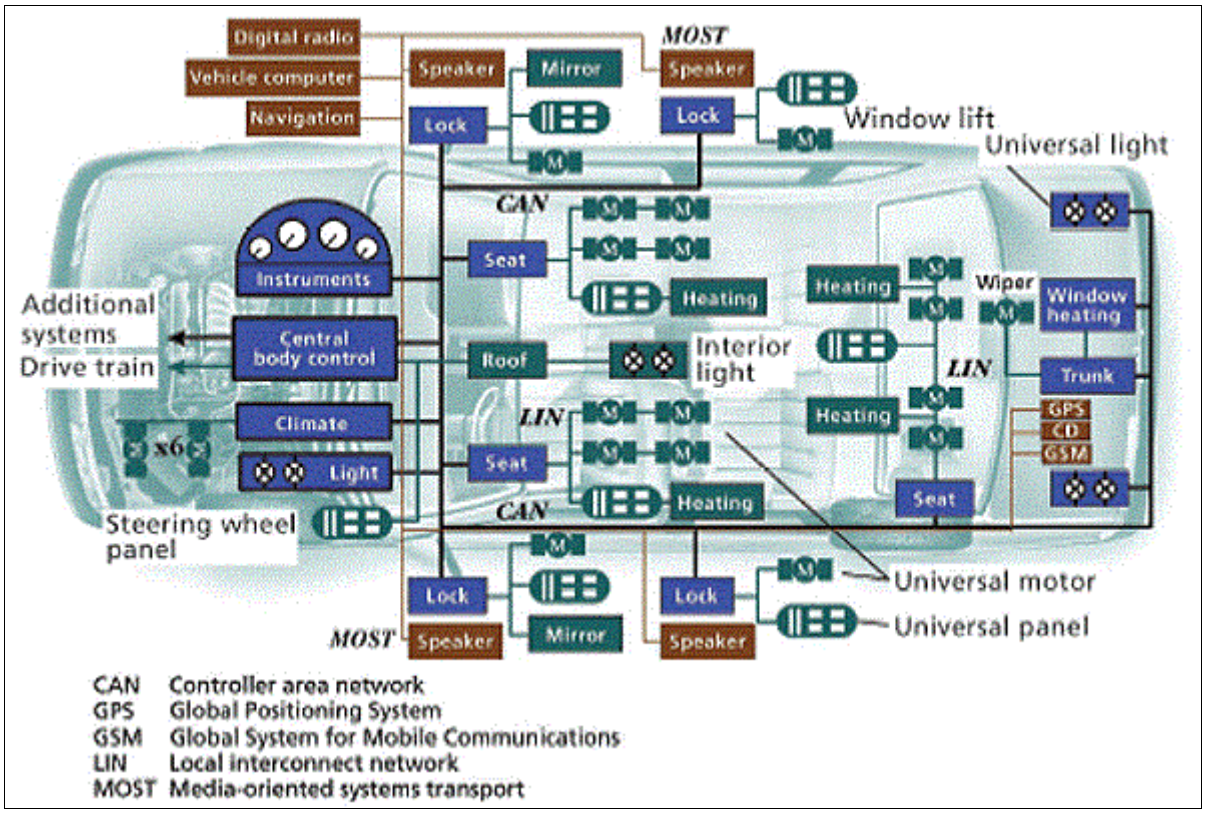

Figure 1. Modern vehicle networks.

[15] CAN Bus Overview, http://en.wikipedia.org/wiki/CAN_bus

[16] OnStar, https://www.onstar.com/us/en/home.html

[17] SYNC 3, http://www.ford.com/technology/sync/

[18] ConnectedDrive, http://www.bmw.com/com/en/insights/technology/connecteddrive/2013/

In larger transportation systems, such as a container ship, the environment is much larger and more complex (see Figure 2). There are dozens of systems that are interdependent and ICS is used to manage these interdependencies. Many of the devices and sensors employed in these large environments are embedded systems that utilize a serial bus to communicate with ICS. This includes the use of CAN bus and other commercial serial networks, such as SAE J1939, to connect CAN bus systems to external devices (e.g., a tractor connected to a trailer).

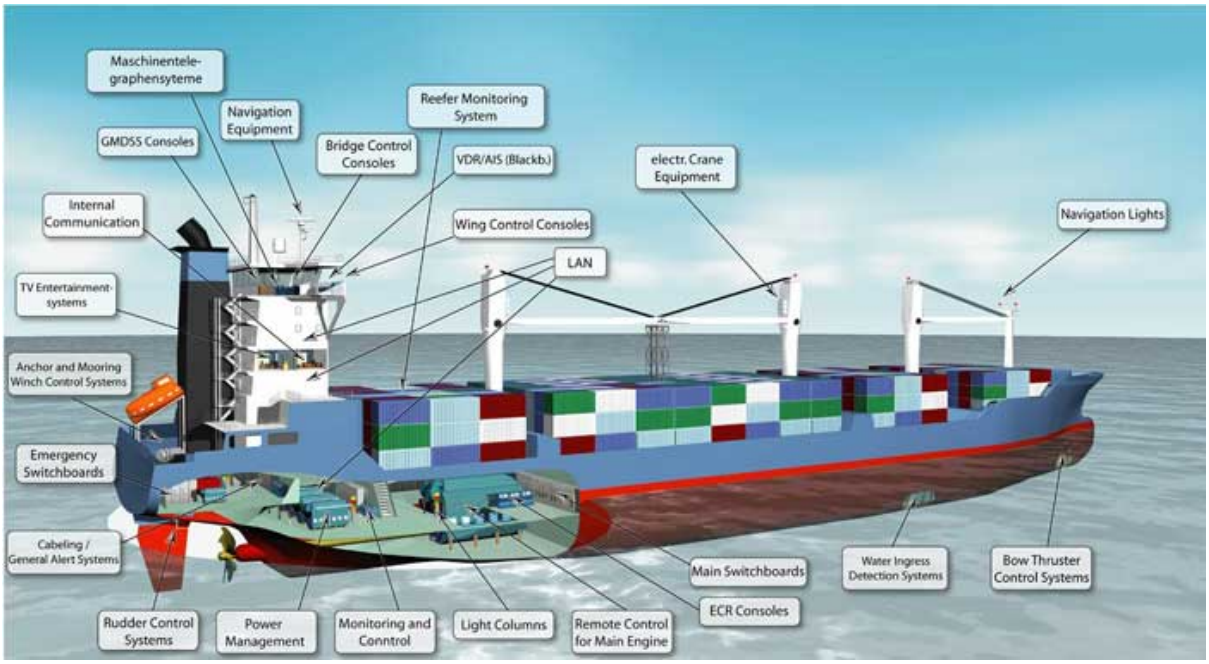

Figure 2. Container ship control systems.

3. Impacts to Facility Security

Although the CAN protocol was primarily developed for automobiles, it has also gained popularity with other industries, transforming the protocol to suit their needs. DeviceNet, created by Allen-Bradley, is strongly based on the CAN protocol and is used in many industries, including nuclear and power generation. PROFIBUS, created by Siemens, is an industrial protocol and, although it is not based on the CAN protocol, it has many major similarities and functionality. The PROFIBUS protocol is used in a number of different industries, including nuclear and power generation. There are many other protocols that are directly based or share major similarities to the base CAN protocol; they inherently share the same weaknesses and vulnerabilities. Cyber attacks against passenger vehicles will not work directly with industrial control systems using similar protocols, but the attacks are similar. The weaknesses and vulnerabilities of these protocols can potentially have a great impact on the control systems used in the nuclear world.

One of the greatest weaknesses of serial networks is that they are designed to operate in a multi-node configuration compared to the single master-slave configuration of RS-232 and RS-485. The design of these networks allows for quick addition of new devices that can all communicate using the same physical media. Bus arbitration and scheduling is handled by the physical layer transceivers. Adding a new CAN bus node to a network simply involves connecting two wires and then setting the proper protocol and baud rate. In a CAN bus

network, there generally is no notion of a sender or receiver address; therefore, messages are just broadcast onto the bus and the interested nodes handle the messages. Because of this design, any node on a CAN bus can broadcast any message, leading to the potential for a compromised node to begin broadcasting messages that may overwrite or replace other node messages.

A potential security vulnerability that can impact nuclear facilities and control systems is wireless mobile devices, including portable electronic devices and vehicles. Portable electronic devices are integrating new wireless capabilities with each release. Bluetooth, GPS, LTE, IR, 802.11, and many more wireless technologies are being integrated into cameras, tablets, cell phones, game consoles, media players, and more. Vehicles have integrated many wireless technologies for convenience, including Bluetooth, LTE, 802.11, GPS, and emerging technologies such as vehicle-to-vehicle.[19] Every electronic device has the potential to be hacked and controlled by an aggressor. Integration of wireless technologies introduces the ability to spread aggressor influence across multiple devices. An employee may have connected his digital camera to his hacked personal computer, introducing camera malware infection. The employee shows vacation pictures to his co-workers while the camera malware is spreading itself, exploiting every wireless capability. The same story could be told of every other personal electronic device, including vehicles. The same camera containing malware could spread to a vehicle over Bluetooth, 802.11, or other means. The vehicle is driven to work and is permitted to pass beyond security boundaries and, if the vehicle is close enough to other wireless devices at or inside the plant, there is potential to spread the malware further.

4. Impacts to Transportation Security

Just as passenger vehicles have seen an increase in electronic devices to improve drivability, safety, and economy of the modern automobile, trucking and security vehicles have also seen an increase in electronically controlled equipment. In many ways, commercial trucking has surpassed the passenger vehicle industry when it comes to integrating technology. In addition to passenger vehicle components, you will find devices for managing trailers, driving time regulation, intricate radio equipment, and Fleet Management Systems. The Fleet Management Systems Interface (FMS) is a standard interface to the CAN bus networks for commercial vehicles. The Fleet Management System interfaces between the vehicle fleet software and the CAN bus networks providing monitoring data. This data collection is remotely available to the transportation company. Additionally, the commercial vehicle industry is investing in and developing autonomous commercial vehicles. In May 2015, Daimler unveiled the Inspiration Truck, which is the first road-legal commercial truck that can drive on its own.[20]

Similar fleet software is often used in security vehicles in order to properly manage and maintain these vehicles. In most cases, fleet software used in security vehicles is also remotely available to the back office, which provides sensitive information such as location and vehicle data. As technology gets better, more and more components are being integrated directly into the security vehicle's internal networks. Ford is releasing the Ford Telematics

---

[19] http://www.its.dot.gov/research/v2v.htm

[20] http://www.theverge.com/2015/5/6/8556791/self-driving-semi-big-rig-freightliner-inspiration-truck

Law Enforcement Edition this year (2015), which more deeply integrates the vehicle's telematics data and fleet management.[21]

Security researchers have already proven that third-party devices connected to vehicles for the purpose of providing additional functionality, such as fleet management services or insurance monitoring, act as gateways between the internet and CAN systems, making them vulnerable to malicious usage. A demonstration of remote vulnerabilities[22] in a device connected to a vehicle CAN bus was illustrated at the S4 Conference[23] in January 2015.

With the addition of fleet management software, autonomous enabling devices, and components more deeply integrated with commercial and security vehicles, additional attack paths and new potential vulnerabilities may exist, even more so than the standard passenger vehicle. Attackers may be able to leverage the additional capabilities and connections provided by commercial and security vehicles and directly attack these vehicles. In addition, possibilities exist that the attacker could attack the fleet management office, taking control of the fleet management system, and potentially attack or greatly influence all fleet vehicles.

Applying this information to the transportation of nuclear material, a possible scenario includes attacking both the transport and escort vehicles. The attack would be possible if the attacker was able to gain physical access to the vehicles for just a few seconds. A remote attack of all vehicles is plausible, but difficult. Once the attack is underway, the transport and escort vehicles would be remotely controlled and disabled, potentially allowing for physical removal of nuclear material. It becomes clear that not only would it be possible to attack a transport through cyber means, but it would be a targeted attack that would be difficult, highly funded, and would take months, possibly years to develop.

5. Mitigation Strategies

Exploitation of a serial network is actually quite trivial because there are no network-level protections provided by any of the protocols discussed in this paper. If a node connected to the network is compromised, then the network is compromised. The challenge involved in creating a complete attack scenario is development of the method for compromising a node connected to the serial network. Historically, this has required physical access to the network (e.g. stuxnet[24]), but remote exploitation is going to quickly become public and more plausible as wireless technologies are integrated. If the remote capabilities for managing a vehicle (e.g., fleet management, OnStar, etc.) are removed, remote exploitation of a vehicle is exponentially more difficult.

One of the major hurdles of trying to secure a serial bus is limitation of the small embedded nodes that are connected to the bus. These devices are designed to be relatively inexpensive and are limited in their processing power. The addition of typical network security technologies, such as encryption or authorization, will require a complete redesign of each

---

[21] http://www.telogis.com/ford/law-enforcement

[22] Progressive Insurance Dongle Security, http://www.forbes.com/sites/thomasbrewster/2015/01/15/researcher-says-progressive-insurance-dongle-totally-insecure/

[23] S4 Conference, http://www.digitalbond.com/s4/

[24] Stuxnet Overview, http://en.wikipedia.org/wiki/Stuxnet

node that is connected to the bus. All nodes on the bus will then have to be configured to communicate using more secure methods; this will increase installation and maintenance costs of operating a serial broadcast network. These changes will have to start with the vendor providing the network enhancements because adding a third-party solution to solve this issue is not very plausible.

Some third-party tools currently being developed will allow for basic monitoring of serial networks to detect malicious activity or physical network issues. These technologies are still young and not yet in production; however, solutions should be available in the near future. The security industry for the embedded systems is becoming more organized each year by working with vendors and original equipment manufacturers to enhance vehicle security.[25]

6. Conclusion

Modern vehicles being used in the nuclear sector are increasingly complex. This complexity comes from the addition of computer systems and communication networks that connect the vehicle to the internet. This is not limited to passenger cars but is also used in large commercial vehicles such as heavy trucks and ships. The integration of computer technology into the vehicles used for critical functions now creates a new potential threat that has not been considered in the past. New procedures are necessary to ensure the protection of vehicle control systems so that cyber security issues will not have an adverse affect on nuclear security. While third-party tools are currently being developed to strengthen cyber security in automobiles, the industry has not broadened the focus to all types of vehicles. Vendors and manufacturers are starting to acknowledge the possible cyber security issues in automobiles and are, at minimum, headed in the right direction to improving security.

REFERENCES

[1] ROBERT BOSCH GAMBH, “CAN Specification Version 2.0,” Stuttgart, Germany 1991.

[2] KOSCHER, K., et al., “Experimental Security Analysis of a Modern Automobile,” University of Washington, Department of Computer Science, Seattle, Washington, 2010.

[3] CHECKOWAY, S., et al., “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” University of California, San Diego, California, 2011.

[4] TRANSPORTATION RESEARCH BOARD, “TRB Special Report 308: The Safety Challenge and Promise of Automotive Electronics: Insights from Unintended Acceleration,” Washington, D.C., 2012.

[5] MARKEY REPORT, “Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk,” Ed Markey: United States Senator, Massachusetts, 2015.

[25] Embedded Security in Cars (ESCAR) USA 2015, https://www.escar.info/escar-usa.html