Survey of Cybersecurity in Automotive Communication Systems

Rodney Pickett & Camille Welcher
Michigan State University

April 14, 2015

Remote data communication is becoming increasingly common in vehicles. Communications are used for a variety of purposes, including infotainment, vehicle status monitoring, traffic congestion mitigation, and even autonomous driving. With so many vehicles being network-aware, and vehicles being potentially dangerous instruments of destruction, it is imperative that security protocols for their communication be studied intensively. This report will survey five different security concerns that will need to be addressed for proper vehicular cybersecurity, providing examples from the literate and discussing mitigation strategies. These security concerns will be divided between Vehicle to Infrastructure and Vehicle to Vehicle communications, though the generality of communications protocols means that some overlap is necessary. Finally, the relevance of some of these concerns will be discussed in the context of the Pedestrian Backup Assist System (PBAS), which has been described in prior literature.

Vehicle to Infrastructure Communication

Vehicle to infrastructure (V2I) communication deals with the processes that allows vehicles to interact with infrastructure equipment such as road side units, radio towers and satellites (Cronin 2014). These structures will be able to connect to a vast number of vehicles and various types of servers. Furthermore, the servers will be capable of collecting sensitive information about drivers and their vehicles. Safety critical information may be distributed across networks in predictable or observable methods (Bin, Marco, and Fei 2013).

Passive Monitoring One major concern for automotive external communication is the privacy of the data between all entities involved. This is particularly true for V2I based communication as the activity between the parties is relatively observable. Attackers with knowledge of the location and specifications of an infrastructure's capability could intercept messages with the proper equipment. This could allow sensitive information about the driver and their vehicle to be accessible. For example, a transportation agency may be looking to collect information about driving habits of individuals based on personal data such as age, race, and other characteristics. If that information was also accompanied with the vehicle information such as make, model, and operational performances, attackers could easily track and target individuals for various criminal activities. Consequently, this will likely cause a decrease in the reputation of the services offered (Klimke 2014).

In order to prevent essential data from being compromised, all information must be encrypted so that only authorized entities are allowed to view the data. However, key exchange is difficult given that vehicles

must connect to various structures as they move geographically. Encryption must be handled with care so that key diversity and exchange efficiency are maximized. Therefore, advanced encryption methods may need to be developed for this discipline. Research findings have shown that it may be possible to generate encrypted keys using unique spatial and time diversities between entities on a network (Bin, Marco, and Fei 2013).

Data Modification Data modification in V2I communication proposes a serious threat in many aspects. The most concerning would be the modification of data that could effect system integrity. Currently, automotive companies can update their latest vehicle systems through wireless connections. These updates can impact safety critical aspects of the system and if they were maliciously modified could have detrimental effects on vehicle performance and behavior [lotfio_towards_2013]. Attackers capable of modifying the update data could do so even if the data was encrypted. As any erroneous data could cause system failure and result in deaths, injuries or damages.

Communication integrity must be used to deal with message tampering between entities, especially when coming from prominent servers such as the manufacture. Protection could be implemented using message authentication techniques, as well as restricting delivery methods based on message content [hideaki2013]. In addition, data may need to be verified in timely manner before it is allowed to effect the system. This will allow the system to reject data safely if tampering is detected (Kyusuk et al. 2014).

Malicious Base Stations Arguably the most important aspects for secure communication are entity authentication and authorization. Vehicles will have the capability of connecting with other entities through various mediums. Connections will require authentication methods in order to properly determine who is trying to communicate with system. In addition, authorization of those trying to communicate with the system must be verified. System integrity must be protected from malicious activity that can be propagated through the different mediums. This principle is similar to other computing platforms such as computers and mobile devices. However, V2I cases must be more restrictive due to the high assurance nature of the automotive industry. Unauthorized access to a vehicles system could allow for partial or complete control of vehicles to remote entities.

It is possible for attackers to set up makeshift road side units that fabricate messages to unsuspecting vehicles. The trouble with this security concern is its potential ease for attackers to set up trap sites using easily obtainable elements such as household routers. In addition, the algorithms and equipment used must be highly efficient and robust as attackers will gain considerable advantages in computing power and familiarity as the components age (Bin, Marco, and Fei 2013). Detecting and mitigating these types of attacks may require multi-level authentication measures and packet filtering techniques performed by dedicated security controllers (Hideaki et al. 2013).

Attacks on Third-Party Devices Add-on devices for remotely monitoring vehicle data are becoming increasingly popular. These devices plug into the On Board Diagnostic port (OBDII or OBD2), which has access to the entire CAN bus. They generally use a cellular network protocol such as 4G LTE to communicate data back to a central server, and most importantly, to receive software updates. Because a) the OBD2 port has direct access to the CAN, b) the CAN protocol includes no validation, and c) there is remote updating capability, such a system provides an ideal attack vector, and opens up the possibility to compromise all essential vehicle functions.

An actual example of such an attack was demonstrated first by Argus Cyber Security. The team showed how a device meant for gathering safety data, called Zubie, could be compromised with a man in the middle attack, enabling an attacker to load arbitrary code (Fox-Brewster 2014). The attack relied on the fact the device did not use HTTPS, instead using the insecure HTTP, and that software updates to the device were not

digitally signed (Ofir and Kapota 2014). The authors harnessed this vulnerability by setting up a malicious base station that would intercept a cellular signal from the device and pretend to the update server; they were then able to load their own code and effectively take control of the device. A similar attack was performed several months later by a different team on a monitoring dongle issued by Progressive Insurance called SnapShot. This dongle is installed in over two million vehicles, and according to the author in (Fox-Brewster 2015):

> "The firmware running on the dongle is minimal and insecure. It does no validation or signing of firmware updates, no secure boot, no cellular authentication, no secure communications or encryption, no data execution prevention or attack mitigation technologies... basically it uses no security technologies whatsoever."

In both these cases, the primary asset to be protected is access to the CAN bus. If the CAN bus is compromised, almost any action can be taken upon the vehicle, including engine and braking control; such a breach directly compromises driver safety. A secondary asset is private information. An attacker could passively monitor all vehicle information and collect that information remotely using the compromised dongle as a server, which could expose personal information about the driver. These assets are primarily threatened by malicious actors performing man in the middle attacks on unsecured add-on devices. The risk to driver safety is likely to only increase with time, as more vehicles make use of such devices, and given the how much control an attacker is given by such an attack, the potential damage is substantial; however, because the man in the middle attack requires considerable resources to implement, and because of the great diversity in CAN protocols between vehicle makes and models, the risk is somewhat lowered.

Fortunately, there are simple and well-tested protocols to avoid man in the middle attacks. Both examples relied on a complete lack of authentication and encryption; further details are in the sections on Data Modification and Malicious Base Stations, and are described in (Bin, Marco, and Fei 2013) and (Kyusuk et al. 2014). The main challenge will be ensuring that all such devices implement these basic procedures as they continue to proliferate. Given how widely used SnapShot is, and the resources behind the company responsible for it, it seems likely that devices produced by even smaller and less regulated manufacturers will continue to be vulnerable for some time.

Vehicle to Vehicle Communication

Vehicle to vehicle, or V2V, communication has been proposed as a way of enabling a distributed traffic information system through propagation of sensor data directly between vehicles. Such a system is referred to as a Vehicular Ad-hoc Network, or VANET. The standard protocol for V2V communication has been previously defined as 802.11p, which has a range of approximately 300 meters and is designed to function properly at high speeds (Hiertz et al. 2010). VANETs open of vehicles to a number of specialized attacks, whether those attacks aim to reduce network integrity or whether they take advantage of a vehicle's individual communications ability.

Distributed Denial of Service Distributed networks are vulnerable to attacks on the integrity of the network itself. One such attack method is the distributed denial of service (DDoS) attack; DDoS attacks are common on the internet, and are well-studied and understood. In the general case, a DDoS attack is carried out by flooding a particular server or sub-network with more traffic than the server or routing software can handle, causing software failure and denying service to the affected individual, institution, or region. In the context of a VANET, a DDoS attack would make use of compromised autonomous vehicles to disrupt the congestion control system and prevent traffic from flowing optimally, or at all, in a targeted region (Garip et al. 2015).

This attack relies on autonomous vehicles to have been previously infected with malicious code (which is demonstrated in other work). Once enough vehicles are infected, they are made to provide false traffic

information suggesting that certain routes are overly congested, which encourages the routing scheduler to choose a particular route or set of routes for many vehicles. By also sending out insincere data from the targeted route suggesting it is more clear than it actually is, and spoofing the time stamps to help prioritize that data, the attack could effectively fool the scheduler into crippling a targeted region. In a possible future scenario where most or all vehicles are autonomous, this could lead to significant economic and safety concerns: workers would be unable to get to their shifts on time, emergency responders might be unable to reach an accident or crime scene, or a particular driver could be physically attacked while immobilized.

A number of mitigation strategies might be pursued. The first is improving authentication schemes, such as with a key system as described earlier in this report. This would allow a more explicit mechanism to disregard vehicles that are found to be bad actors. Unfortunately, a DDoS could be carried out without bringing great attention to individual actors, so long as the attackers are willing to accept a slower response time and less efficacy (Garip et al. 2015). In addition to authentication and a means to ignore known bad actors, such a congestion control scheme should make use of cloud-based or V2I congestion control mechanisms, such as those provided by Google using cellular data. While cloud-based systems suffer from slow response time, their data would be a valuable prior to identify outliers in the VANET and ultimately ignore bad actors.

Security Concerns in the PBAS System

The pedestrian backup system presented to the team requires interacting with the braking subsystem. The actual management between the systems is outside the scope of the system, however the backup system will be connected to the media center that most likely exists within the vehicle. Most media centers allow for passengers to plug in devices for various applications. This interaction between systems could allow hackers to upload malicious programs onto personal devices that remain dormant until plugged into a vehicle. Once connected, the programs may modify the system behavior or critical data. Therefore, this process could inadvertently allow indirect control to the braking subsystem. This occurrence is critical since braking in various driving conditions could lead to death and injuries to passengers and pedestrians. In addition, this will allow hackers the ability to control traffic and potentially cause property damage. Fortunately, with proper privilege management on all subsystem inputs, outputs, and manipulated data this type of attack could possibly be prevented.

A further risk is essentially a denial of service attack. One could imagine any number of ways to trip the cushion described by our system and effectively render the vehicle immobile: CAN bus access could be used to produce a false critical warning signal, or even send a message explicitly asking the cushion to be inflated; or an attacker could make use of physical interference to activate the alarms, perhaps by occluding the sensors with a material which reflects electromagnetic signals. One way this attack could be mitigated would be allowing the driver to manually disable the cushion depending on the circumstances, using a physical switch. Additionally, the ECU should have on-board logic to detect outliers and prevent deployment under suspicious circumstances. Many attacks in general rely on the lack of authentication and validation for devices on the CAN bus, so much of the risk can be effectively mitigated by placing as validation on the individual ECU's themselves, outside the attackers' reach.

References

Bin, Z., G. Marco, and H. Fei. 2013. "Key Agreement Algorithms for Vehicular Communication Networks Based on Reciprocity and Diversity Theorems." In *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY*. Vol. 62. series 8.

Cronin, Brian. 2014. "Vehicle-to-Infrastructure (V2I) Communications for Safety." ITS Joint Program Office. http://www.its.dot.gov/research/v2i.htm.

Fox-Brewster, Thomas. 2014. "Zubie: This Car Safety Tool 'Could Have Given Hackers Control Of Your Vehicle'." *Forbes* (November). http://www.forbes.com/sites/thomasbrewster/2014/11/07/car-safety-tool-could-have 2/.

———. 2015. "Hacker Says Attacks On 'Insecure' Progressive Insurance Dongle In 2 Million US Cars Could Spawn Road Carnage." *Forbes* (January). http://www.forbes.com/sites/thomasbrewster/2015/01/15/researcher-says-progressive-insurance-dongle-totally-insecure/.

Garip, Mevlut Turker, Mehmet Emre Gursoy, Peter Reiher, and Mario Gerla. 2015. "Congestion Attacks to Autonomous Cars Using Vehicular Botnets." In Internet Society. doi:10.14722/sent.2015.23001. http://www.internetsociety.org/doc/congestion-attacks-autonomous-cars-using-vehicular-botnets.

Hideaki, K., K. Chisato, K. Makoto, and N. Manabu. 2013. "Approaches for Vehicle Information Security." INFORMATION-TECHNOLOGY PROMOTION AGENCY.

Hiertz, Guido, Dee Denteneer, Lothar Stibor, Yunpeng Zang, Xavier Costa, and Bernhard Walke. 2010. "The IEEE 802.11 Universe." *IEEE Communications Magazine* 48 (1) (January): 62–70. doi:10.1109/MCOM.2010.5394 http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5394032.

Klimke, Martin. 2014. "Benefits and Values of the Trusted Platform Module in the Automotive Industry." Infineon Technologies.

Kyusuk, H., P. Swapna, S. Kang, and W. Andre. 2014. "Practical Real-Time Frame Authentication for In-Vehicle Networks." University of Michigan.

Ofir, Ron, and Ofer Kapota. 2014. "A Remote Attack on an Aftermarket Telematics Service." *Argus Cyber Security Blog*. http://argus-sec.com/blog/remote-attack-aftermarket-telematics-service/.