Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities

Mohamed Amin and Zaid Tariq

> “ *To know is to control.* ”
>
> Ishmael Scott Reed
> Poet, essayist, and novelist

Today's vehicles depend on numerous complex software systems, some of which have been developed by suppliers and must be integrated using "glue code" so that they may function together. However, this method of integration often introduces cybersecurity vulnerabilities at the interfaces between electronic systems. In this article we address the “glue code problem” by drawing insights from research on supplier-manufacturer outsourcing relationships in the automotive industry. The glue code problem can be framed as a knowledge coordination problem between manufactures and suppliers. Car manufacturers often employ different levels of intrusiveness in the design of car subsystems by their suppliers: the more control over the supplier the manufacturer exerts in the design of the subsystem, the more intrusive the manufacturer is. We argue that high intrusiveness by car manufacturers in defining module interfaces and subcomponents for suppliers would lead to more secure cars.

Introduction

The modern car is increasingly dependent on electrical and software systems. A modern vehicle has anywhere from 30 to 70 electronic control units that monitor and control its different subsystems (Studnia et al., 2013a), which are integrated using "glue code" (Checkoway et al., 2011). The glue code enables car manufacturers to outsource the development of particular systems and subsystems, which are then integrated when the car is assembled.

However, within and between these modules, several cybersecurity vulnerabilities in the modern car have been identified and documented by researchers. Examples include vulnerabilities in sound systems, Bluetooth modules, onboard diagnostics systems, cellular communications, and the bus connecting electronic control units, (Checkoway et al., 2011; Eichler, 2007; Hoppe et al., 2009; Koscher et al., 2010; Raya & Hubaux, 2007; Wolf et al., 2004). Practitioners have also stressed how vulnerable the modern car is to cyber-attacks (Miller & Valasek, 2013; Venturebeat, 2013; Yadron, 2014). Both local and remote attacks have been documented (Studnia et al., 2013a). Theft, electronic tuning, sabotage, and surveillance are among the goals of those who cyber-attack cars (Studnia et al., 2013a). Most vulnerabilities in the modern car arise from incorrect assumptions made by the glue code that calls functions on different electronic control units (Checkoway et al., 2011). These incorrect assumptions may occur at the subcomponent level as well as the interface level.

Checkoway and colleagues (2011) argue that the true source of the glue code problem can be traced back to the setup of the ecosystems used to manufacture cars. Auto manufacturers build ecosystems to outsource digital systems in the same way that they outsource mechanical parts. Although every supplier tests their modules, security vulnerabilities usually arise when those modules are subsequently integrated by the car manufacturers. Outsourcing module design may introduce security vulnerabilities at the interface between modules and the car (i.e., in the glue code), as well as between distinct modules designed by external suppliers. The latter source of vulnerabilities is caused by feature interaction problems between different modules and this source of vulnerabilities is outside the scope of this article.

By analyzing various security solutions that have been proposed to improve the overall security of the modern car (Bouard et al., 2013; Herrewege, et al., 2011; Studnia et al., 2013a; Stumpf et al., 2009; Wolf & Gendrullis, 2012; Wolf & Weimerskirch, 2004), we observe that the proposed solutions: i) only focus on providing technical architectures of security solutions, ii) would typically require substantial changes to existing implementation processes in the automobile industry, and iii) do not directly address the glue code problem identified by Checkoway and colleagues (2011). To address these shortcomings, we examined literature on manufacturer-supplier relationships. As will be described below, we identified that the manufacturer's level of intrusiveness in supplier design could aid in solving the interface boundary, or glue code, problem. In particular, we argue that, for manufacturers to avoid security vulnerabilities at the boundaries between electronic control units, they should be highly intrusive in the supplier design of the module interfaces and subcomponents that call other electronic control units in the car.

In the following section, we describe the proposed cybersecurity solutions for cars and existing manufacturer-supplier relationships. Next, we examine an existing analytical framework and propose our solution. We close by outlining our contribution and offering conclusions.

Proposed Solutions

Three broad categories of solutions have been proposed by various researchers: i) encryption of communications, ii) anomaly detection, and iii) improved integrity of the embedded software (Studnia et al., 2013a). Table 1 summarizes representative solutions and their salient features.

Car manufacturers have been increasingly outsourcing module design (Calabrese & Erbetta, 2005). Suppliers organize themselves around manufacturers' facilities geographically to form supplier parks (Collins et al., 1997; Larsson, 2002; Volpato, 2004). In addition to geo-

Table 1. Representative cybersecurity solutions for the modern car

Security Solution	Salient Features
Proxy-Based Security Architecture for CE Device Integration (Bouard et al., 2013)	• Proxy-based IP security solution to secure consumer electronic devices able to access a car's onboard network. • Enforces communication decoupling between internal and external networks by using a security proxy. • Approach requires partial redesign of electronic control units to support in-band signaling between the control units and the security proxy.
Multipurpose Electronic control Units and Hardware Security Module (Stumpf et al., 2009; Wolf & Gendrullis, 2012)	• A dedicated hardware security module governs all traffic between electronic control units and authenticates individual frames. • Hardware security module is then implemented in a system that uses the concept of virtualization to centralize all electronic control units in a car onto a single virtual machine • Integrates inherent features of virtual machines: integrity, trustworthiness, and authenticity.
Security in Automotive Bus Systems (Wolf et al., 2004)	• Secure the existing in-car network using controller authentication, encrypted communication and gateway firewalls. • Inter Bus communication happens through a central authentication and encryption gateway on each bus.
CANAuth (Herrewege et al., 2011)	• Backward-compatible controller area network (CAN) authentication protocol designed using hashed message authentication code (HMAC). • This protocol uses the existing CAN bus and forms an additional layer on top of the existing protocol.
Intrusion Detection System (Studnia et al., 2013b)	• Automotive security using an intrusion detection system for the CAN bus.

graphic allocation, smaller suppliers usually form a hierarchy behind large first-tier suppliers forming around car manufacturers (Volpato, 2004). Knowledge and task partitioning differ depending on the relationships between supplier and manufacturer (Cabigiosu et al., 2013; Zirpoli & Camuffo, 2009) as well as the nature of the product being co-developed (Takeishi, 2002). Manufacturers and suppliers co-develop modules with varying levels of intrusion by the manufacturer in the supplier design (Cabigiosu et al., 2013).

The Manufacturer-Supplier Co-Development Approach

Cabigiosu and colleagues (2013) compared two similar vehicle component co-development projects carried out by the same first-tier supplier with two different automakers. They used an analytical framework to analyze the manufacturer’s approach to supplier integration in product development. The results showed that the two manufacturers employed different levels of "intrusiveness" in supplier design. Manufacturer intrusiveness represents the level of detail and the amount of coordination the manufacturer employed in defining the design of the respective artifact. An intrusive approach to the co-development is an approach where the manufacturer exerts high level of control over the supplier’s design decisions. The level of intrusiveness influences the knowledge the manufacturer has about the interface and the subcomponents of the module. Analyzing the two different approaches reported by Cabigiosu and colleagues (2013), and the corresponding degrees of intrusiveness with each approach, leads to insights on how the glue code problem may arise and what car manufacturers can do to prevent it.

According to Cabigiosu and colleagues (2013), manufacturers engage with suppliers at different levels of intrusiveness in:

1. *Module-to-car system-level design:* includes functional and performance parameters that the module has to adhere to in order for it to comply with overall functional and performance parameters of the car as a whole.

2. *Module-to-module interface design*: includes protocol-level functionality that the module has to adhere to in order for it to interoperate with various other modules in the car.

3. *Individual-subcomponent-to-module system-level design:* includes functional and performance parameters that various subcomponents in the module have to adhere to for the module to work as a whole.

4. *Individual subcomponents design:* functional- and protocol-level parameters that subcomponents have to adhere to.

Table 2 compares the approaches taken by two manufacturers in co-developing an air conditioning system with the same supplier (Cabigiosu et al., 2013). Manufacturer A’s approach can be characterized as intrusive whereas manufacturer B’s approach can be characterized as non-intrusive.

Table 2. Comparison between intrusive and non-intrusive approaches to manufacturer-supplier co-development (Cabigiosu et al., 2013)

	Manufacturer A’s Approach (Intrusive)	**Manufacturer B’s Approach (Non-Intrusive)**
Interface definition	• Stable and detailed • Definitions frozen before design starts • Specifics are clear, easy to follow, and do not change	• Fluid and changing • Set the main concept and architecture but allow supplier to suggest design
Co-development approach	• Formal information-sharing sessions monthly and bi-weekly • Daily communications, sometimes face to face • Mainly to sort out component interdependencies	• Heavily outsourced engineering tasks to supplier. • Used a standard codified co-development practice • Used rigid systems and procedures
Knowledge partitioning	• Owned component-specific knowledge	• Did not own component-specific knowledge

The glue code problem can be seen as a knowledge coordination problem. Suppliers design components based on performance and functional specifications provided by the manufacturer. Design decisions can sometimes be left to the discretion of the supplier, who may assume that particular components in the car work in certain ways. This was the case with the Airbiquity software component analyzed by Checkoway and colleagues (2011), where they found that the code calling this component and binding it to other telematics functions made the wrong assumptions about the component supported packet size and resulted in a buffer overflow vulnerability. Packet sizes are usually defined as part of the interfaces; given that the car manufacturer did not know the right packet size used by the software component shows that the manufacturer was non-intrusive in defining this interface. An intrusive strategy would avoid such a problem because the manufacturer would know the right packet size because it was the one defining it. Only the manufacturer is in a position that would allow a holistic view of all the different electronic control units and their inner workings. Thus, the glue code problem can be reduced if the manufacturer employs the right level of intrusiveness with different suppliers. We argue that the right level of intrusiveness by a manufacturer for avoiding the glue code problem is being highly intrusive in defining the module interfaces and the inner subcomponents of the electronic control unit module that call other modules in the car. This degree of intrusiveness in the manufacturer-supplier relationship is similar to a hybrid-control governance model of open source platforms (Noori & Weiss, 2013), where increased control yields higher quality but does require greater effort in the form of overseeing all the parties involved. Where increased quality equates to increased security, this added effort will be worthwhile.

Conclusion

As described earlier, security solutions can by broadly divided into three main categories: i) encryption of communications, ii) anomaly detection, and iii) integrity of the embedded software, where the final category refers to approaches that ensure the car's critical software is not affected by a cyber-attack (Studnia et al., 2013). Our contribution adds to this third category by identifying the manufacturer-supplier relationship that reduces the risk of vulnerabilities at the boundaries between electronic control units and thus protects the integrity of the car's critical software modules.

Our contribution allows car manufacturers to employ the right level of intrusiveness in their supplier design to increase the level of cybersecurity in their cars. It allows individuals responsible for leading engineering efforts at both manufacturer and supplier organizations and individuals controlling manufacturer-supplier inter-firm relations to pick the right working model for building secure cars. We encourage the research community to further explore manufacturer-supplier relationship theory and other managerial theories in their search for a solution to securing the car.

Manufacturers can choose the optimal degree of intrusiveness when co-developing new products with their suppliers. We argue that an intrusive strategy can be employed by manufacturers when developing electronic control units to reduce the risk of cybersecurity vulnerabilities at the boundaries between systems. We invite further research into this domain to tackle the cybersecurity problems of the modern car. Future work could empirically test our claim that increased manufacturer intrusiveness in supplier design leads to more secure cars.

About the Authors

Mohamed Amin is an MASc student in the Technology Innovation Management program at Carleton University in Ottawa, Canada. His research interests include cybersecurity, API strategy, and industry architecture. He works as a Solution Architect for Alcatel-Lucent Canada, where he designs and delivers network solutions for various internet service providers around the world.

Zaid Tariq is completing his MEng in Technology Innovation Management at Carleton University in Ottawa, Canada. He also holds a BEng degree in Computer Engineering from McGill University in Montreal, Canada. He is a Senior Network Engineer at Cisco Systems and has 9 years experience working in the network design, architecture, and test domains.

Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities

Mohamed Amin and Zaid Tariq

References

Bouard, A., Schanda, J., Herrscher, D., & Eckert, C. 2013. Automotive Proxy-Based Security Architecture for CE Device Integration. In P. Bellavista, C. Borcea, C. Giannelli, T. Magedanz, & F. Schreiner (Eds.), *Mobile Wireless Middleware, Operating Systems, and Applications:* 62–76. Berlin: Springer Berlin Heidelberg.

Cabigiosu, A., Zirpoli, F., & Camuffo, A. 2013. Modularity, Interfaces Definition and the Integration of External Sources of Innovation in the Automotive Industry. *Research Policy,* 42(3): 662–675. http://dx.doi.org/10.1016/j.respol.2012.09.002

Calabrese, G., & Erbetta, F. 2005. *Outsourcing and Firm Performance: Evidence from Italian Automotive Suppliers.* Paper presented at the 13th Annual IPSERA Conference. Catania: Universita di Catania.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Patel, S., Roesner, F., Czeskis, A., & Kohno, T. 2011. *Comprehensive Experimental Analyses of Automotive Attack Surfaces.* Paper presented at the USENIX Security Symposium. San Francisco: USENIX Association.

Collins, R., Kimberly, B., & Pires, S. 1997. Outsourcing in the Automotive Industry: From JIT to Modular Consortia. *European Management Journal, 15(5):* 498–508. http://dx.doi.org/10.1016/S0263-2373(97)00030-3

Eichler, S. 2007. A Security Architecture Concept for Vehicular Network Nodes. In *Proceedings of the 6th International IEEE Conference on Information, Communications & Signal Processing:* 1–5. Washington, DC: IEEE. http://dx.doi.org/10.1109/ICICS.2007.4449730

Herrewege, A., Singelee, D., & Verbauwhede, I. 2011. *CANAuth: A Simple, Backward Compatible Broadcast Authentication Protocol for CAN Bus.* Paper presented at the ECRYPT Workshop on Lightweight Cryptography. Louvain-la-Neuve, Belgium: ECRYPT.

Hoppe, T., Kiltz, S., & Dittmann, J. 2009. Automotive IT Security as a Challenge: Basic Attacks from the Black Box Perspective on the Example of Privacy Threats. In *Computer Safety, Reliability, and Security – Lecture Notes in Computer Science, 5575:* 145–158. Berlin: Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-04468-7_13

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., & Savage, S. 2010. Experimental Security Analysis of a Modern Automobile. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy:* 447–462. Oakland, CA: IEEE.

Larsson, A. 2002. The Development and Regional Significance of the Automotive Industry: Supplier Parks in Western Europe. *International Journal of Urban and Regional Research,* 26(4): 767–84. http://dx.doi.org/10.1111/1468-2427.00417

Miller, C., & Valasek, C. 2013. *Adventures in Automotive Networks and Control Units.* Paper presented at DEF CON 21 Hacking Conference. Las Vegas, NV: DEF CON.

Noori, N., & Weiss, M. 2013. Going Open: Does it Mean Giving Away Control? *Technology Innovation Management Review,* 3(1): 27-31. http://timreview.ca/article/647

Raya, M., & Hubaux, J. P. 2007. Securing Vehicular Ad Hoc Networks. *Journal of Computer Security,* 15(1): 39–68.

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., & Laarouchi, Y. 2013a. A Survey of Security Threats and Protection Mechanisms in Embedded Automotive Networks. In *Proceedings of the 2nd Workshop on Open Resilient Human-Aware Cyber-Physical Systems (WORCS-2013).* Budapest, Hungary: IEEE. http://dx.doi.org/10.1109/DSNW.2013.6615528

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., & Laarouchi, Y. 2013b. Security of Embedded Automotive Networks: State of the Art and a Research Proposal. In *Proceedings of 2nd Workshop on Critical Automotive Applications: Robustness & Safety of the 32nd International Conference on Computer Safety, Reliability and Security.* Toulouse, France: SAFECOMP.

Stumpf, F., Meves, C., Weyl, B., & Wolf, M. 2011. *A Security Architecture for Multipurpose ECUs in Vehicles.* Paper presented at the 25th Joint VDI/VW Automotive Security Conference. Ingolstadt, Germany.

Takeishi, A. 2002. Knowledge Partitioning in the Interfirm Division of Labor: The Case of Automotive Product Development. *Organization Science,* 13(3): 321–338. http://dx.doi.org/10.1287/orsc.13.3.321.2779

VentureBeat. 2013. Ford Wants You to Join It in Hacking Car Software and Hardware. *VentureBeat.* Accessed January 10, 2015: http://venturebeat.com/2013/11/06/ford-wants-you-to-join-it-in-hacking-car-software-and-hardware-video/

Volpato, G. 2004. The OEM-FTS Relationship in Automotive Industry. *International Journal of Automotive Technology and Management,* 4(2/3): 166–197. http://dx.doi.org/10.1504/IJATM.2004.005325

Weimerskirch, A. 2012. *Automotive and Industrial Data Security.* Paper presented at the Cybersecurity for Cyber-Physical Systems Workshop. Ann Arbor, MI: National Institute of Standards and Technology.

Wolf, M., & Gendrullis, T. 2012. Design, Implementation, and Evaluation of a Vehicular Hardware Security Module. In H. Kim (Ed.), *Information Security and Cryptology-ICISC:* 302–318. Berlin: Springer Berlin Heidelberg.

Wolf, M., Weimerskirch, A., & Paar, C. 2004. *Security in Automotive Bus Systems.* Paper presented at Workshop on Embedded Security in Cars (ESCAR 2004). Bochum, Germany: ESCAR.

Yadron, D. 2014. Tesla Invites Hackers for a Spin. *The Wall Street Journal Blog.* Accessed January 10, 2015: http://blogs.wsj.com/digits/2014/08/08/telsa-invites-hackers-for-a-spin/

Zirpoli, F., & Camuffo, A. 2009. Product Architecture, Inter-Firm Vertical Coordination and Knowledge Partitioning in the Auto Industry. *European Management Review,* 6(4): 250–264. http://dx.doi.org/10.1057/emr.2009.25

Citation: Amin, M., & Tariq, Z. 2015. Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities. *Technology Innovation Management Review,* 5(1): 21–25. http://timreview.ca/article/863

Keywords: cybersecurity, vulnerabilities, automobile manufacturing, car design, supplier, outsourcing, control, governance, supplier-manufacturer relationships, glue code, intrusiveness