Towards a Fail-Operational Intrusion Detection System for In-Vehicle Networks

Clinton Young, Joseph Zambreno
Department of Electrical and Computer Engineering
Iowa State University
{cwyoung,zambreno}@iastate.edu

Gedare Bloom
Department of Electrical Engineering and Computer Science
Howard University
gedare.bloom@howard.edu

***Abstract*—The landscape of automotive in-vehicle networks is changing driven by the vast options for infotainment features and progress toward fully-autonomous vehicles. However, the security of automotive networks is lagging behind feature-driven technologies, and new vulnerabilities are constantly being discovered. In this paper, we introduce a road map towards a security solution for in-vehicle networks that can detect anomalous and failed states of the network and adaptively respond in real-time to maintain a fail-operational system.**

I. Introduction and Problem Statement

Recent trends in industry towards smart and interconnected devices, referred to as the Internet of Things are now also appearing in the automotive world. Passenger comfort and infotainment features continue to progress through the advancement of in-vehicle networks and connectivity of the automotive system with its environment. However there is a lack of security to prevent comfort and efficiency features from compromising safety-critical control systems. Examples of such security vulnerabilities include the now infamous Jeep Grand Cherokee hack [1], and more recently the remote hack of a Tesla Model S covered on Wired.com.

The automotive industry has slowly replaced much of the mechanical couplings between car components with electronics and software, because electronics are cheaper and lighter than their mechanical counter parts. In conjunction with the hardware, an automobile also contains over 100 million lines of software [2], and consumers are constantly seeking features that allow for more interaction between smart phones and car. Automotive in-vehicle networks are rapidly changing because of consumer demand for the interconnectivity of devices, and what had previously been a network isolated from attackers due to the limited possible access points is now more vulnerable. Having a wireless access point in the in-vehicle network allows for remote diagnostics and over-the-air firmware updates to thousands of vehicles simultaneously, but at a cost: safety and security vulnerabilities are introduced to what was once a closed system.

Our primary goal is to solve security problems inherent with in-vehicle networks that mix safety-critical packets with non-critical messages, such as those for ADAS and infotainment. We propose a fail-operational intrusion detection system (FO-IDS) that identifies potential attacks and causes the cyber physical system (CPS) to transition to an operational safe state.

This material is based upon work supported by the National Science Foundation under Grant No. CNS 1646317 and CNS 1645987.

II. Related Work

The idea of intrusion detection is not new, however it is only recently being applied to automotive in-vehicle networks. IDSs work by monitoring messages and frequencies of the network and system to identifying anomalies and respond accordingly. Currently in safety-critical CPSs, when an anomaly is encountered, the system enters a fail-safe mode; this mode maintains operations while handling the anomaly. The system will return to normal operating modes after the system is clear of any anomalies. However there is a lack of cyber anomaly detection and response in in-vehicle networks. False positives are a major issue in IDSs, and several groups have demonstrated IDS with low to zero false positives [3]. Other work specifically on CPS IDSs focuses on different methods of anomaly detection. Few of these necessarily perform well for automotive in-vehicle networks, and a method of detecting anomalies using the fail-operational system needs to be developed.

SecureCore [4] and Secure System Simplex Architecture [5] introduce time-based anomaly detection for CPS IDS that revisits the Simplex architecture by using redundant hardware controllers. Their solution works at the processor level, and it can detect and recover from attacks that under- or over-use processor time. Translating this solution to defend in-vehicle networks is not straightforward, because malicious packets can take the same amount of time to process as benign ones.

Sasaki et al. [6] introduce a framework to detect man-in-the-middle attacks and switch to a backup control system, which could be useful to help generate a fail-operational mode.

We aim to leverage previous work in regards to IDS and suggest features for anomaly detection while continuing to explore other designs and better understand the characteristics of an IDS in real-world automotive CPS. We propose an FO-IDS that identifies security and safety anomalies and finds a fail-operation mode that the system can transition to when an intrusion has been detected.

III. Our Approach

FO-IDS is an improvement to classical automotive IDS solutions that will incorporate information flow tracking and sensor data provenance. Response of the FO-IDS will cause a mode-change in the automotive system to enter a safe, degraded, yet operational state that prevents the detected attack, and then initiate recovery to restore degraded services. Figure 1 shows a high-level conceptual design of our proposed system.

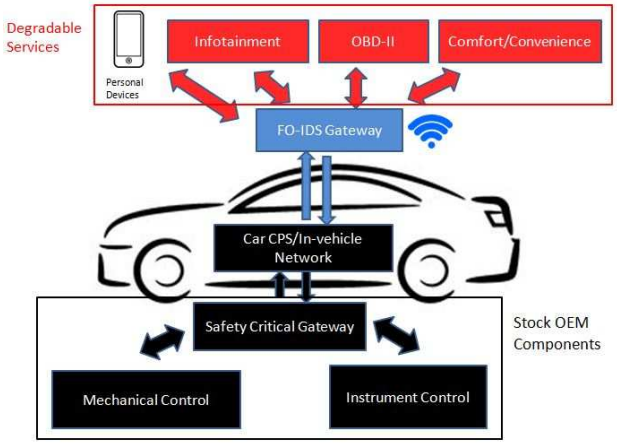

Fig. 1. Project Concept

A. Design Classifiers for Sequential Anomaly Detection

An FO-IDS needs to be able to identify anomalies that occur in sequences and combinations of messages observable at in-vehicle network gateways and ECUs. Sequential anomalies are important for detecting semantic attacks that span multiple state transitions of a CPS, i.e. attacks that may induce seemingly valid individual transitions but invalid, unsafe aggregate transition behavior. A Bluetooth pairing that leads to a malicious firmware upgrade is an example of a sequence-based semantic attack, where infiltration precedes compromise with multiple intervening CPS state transitions. The Bluetooth pairing itself is not anomalous, and neither is a firmware upgrade, but the two together needs to raise suspicion.

In-vehicle networks use shared bus protocols that mix predictable, high-priority, periodic control messages with less predictable, lower priority messages. The IDS will partition the incoming messages to at the IDS to examine control messages using algorithms that exploit the highly predictable nature, while non-control messages will require algorithms that can tolerate more randomness. Kernel-based machine learning appears well-suited to sequential anomaly detection [7] and the high dimensional feature spaces of vehicular data, but can have substantial time complexity. We will investigate whether kernel-based approaches can be efficient enough for IDS at in-vehicle network transmission rates, and will explore sequence mining with heuristic pruning of the state space to include limiting history and prioritizing search paths using physical constraints of the in-vehicle network to parameterize the machine learning algorithms.

B. Improve Classification by Enhancing Feature Collectors

The unmodified in-vehicle network traffic will provide a wealth of data for anomaly detection. However, to improve classifier performance we will increase the available data by tracking, within the constraints of network bandwidth and control unit resources, data provenance and information flows. We will explore the use of device identification in addition to (logical) timestamps that would assist in resisting replay and false data injection attacks. Information flow control and taint tracking will associate device tags with data that propagates through the in-vehicle network to enable traditional information security approaches such as Biba and Bell-LaPadula to be used between automotive subsystems.

C. Recoverable Fail-Operational Modes

Much work exists in fail-operational vehicular control to ensure fail-operational safety in the transition to fly-by-wire avionics [8]. Our aim is to understand the nature of each in-vehicle network component with respect to its capability to fail gracefully, which components are naturally able to fail into an operational state, and which require additional support from fault tolerance mechanisms. We will create a taxonomy of in-vehicle components (gateways, ECUs, and subnetworks) with respect to their fail-operational capability, and investigate mechanisms such as real-time microrebooting and network partition-tolerance to enable fail-operational responses when anomalies are detected.

References

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *2010 IEEE Symposium on Security and Privacy*, May 2010, pp. 447–462.

[2] R. N. Charette, "This car runs on code," *IEEE spectrum*, vol. 46, no. 3, p. 3, 2009.

[3] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *2010 Sixth International Conference on Information Assurance and Security (IAS)*, Aug. 2010, pp. 92–98.

[4] M. K. Yoon, S. Mohan, J. Choi, J. E. Kim, and L. Sha, "SecureCore: A multicore-based intrusion detection architecture for real-time embedded systems," in *Real-Time and Embedded Technology and Applications Symposium (RTAS), 2013 IEEE 19th*, Apr. 2013, pp. 21–32.

[5] S. Mohan, S. Bak, E. Betti, H. Yun, L. Sha, and M. Caccamo, "S3a: Secure System Simplex Architecture for Enhanced Security and Robustness of Cyber-physical Systems," in *Proceedings of the 2Nd ACM International Conference on High Confidence Networked Systems*, ser. HiCoNS '13. New York, NY, USA: ACM, 2013, pp. 65–74. [Online]. Available: http://doi.acm.org/10.1145/2461446.2461456

[6] T. Sasaki, K. Sawada, S. Shin, and S. Hosokawa, "Model based fallback control for networked control system via switched Lyapunov function," in *IECON 2015 - 41st Annual Conference of the IEEE Industrial Electronics Society*, Nov. 2015, pp. 002 000–002 005.

[7] V. Chandola, V. Mithal, and V. Kumar, "Comparative Evaluation of Anomaly Detection Techniques for Sequence Data," in *2008 Eighth IEEE International Conference on Data Mining*, Dec. 2008, pp. 743–748.

[8] P. Sinha, "Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives," *Reliability Engineering & System Safety*, vol. 96, no. 10, pp. 1349–1359, Oct. 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S095183201100041X