2022 NDIA MICHIGAN CHAPTER
GROUND VEHICLE SYSTEMS ENGINEERING
AND TECHNOLOGY SYMPOSIUM
CYBERSECURITY OF GROUND SYSTEMS TECHNICAL SESSION
AUGUST 16-18, 2022 - NOVI, MICHIGAN

Assurance and Verification of Vehicular Microelectronic Systems (AV2MS): Supply Chain Assurance through Utilization of Side Channel Radio Frequency Emissions for Improved Ground Vehicle Cybersecurity

Yale Empie[1], Matthew Bayer[1]

[1] Ground Vehicle Systems Center, Warren, MI

ABSTRACT

Modern vehicular systems are comprised of numerous electronics control units (ECUs) that consist of thousands of microelectronics components. Individual ECU systems are reliant upon "trust" in the supply chain for defense. This paper describes an approach utilizing historically offensive-based cybersecurity technology, side-channels, to quantify and qualify malicious ECU states in a bus-agnostic, logically-decoupled method of assurance and verification. Providing a measure of supply chain assurance to end-users.

Citation: Yale Empie, Matthew Bayer, "Assurance and Verification of Vehicular Microelectronic Systems (AV2MS): Supply Chain Assurance through Utilization of Side Channel Radio Frequency Emissions for Improved Ground Vehicle Cybersecurity," In *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium* (GVSETS), NDIA, Novi, MI, Aug. 16-18, 2022.

1. INTRODUCTION

Supply chain has been a major concern for technology end-users across the globe for microelectronics. There are various policies and regulations in the defense industry that work to provide a measure of confidence that the delivered product hasn't been maliciously tampered with. This system ultimately relies upon the idea of "trust" all the way from development to installation.

Modern vehicular systems are comprised of numerous, complex microelectronics systems, known as electronics control units (ECUs). These ECUs govern numerous aspects of a vehicle's operation. They communicate on standardized vehicular data-bus networks such as Controller Area Network (CAN), SAE J1939, or MIL-STD-1553. The data-buses themselves provide minimal protection against malicious cyber threats to the ECUs. This security weakness is exacerbated by multiple intrusion methods and modalities, and as a result, increases in modern vehicle connectivity.

State-of-the-art technologies to detect and defend against malicious cyber threats to ECUs analyze and prevent the effects that broadcast onto the vehicular data-bus network, such as Intrusion Detection and

Prevention (IDPS) systems and Secure Gateways. These cyber defensive technologies are logically and electrically connected to these ECUs via the vehicular data bus. However, these technologies do not identify and protect against latent malicious functionality that is not broadcast on the vehicle data-bus. Thus, becoming a weak point in a vehicle's cybersecurity posture as they analyze and defend against only what they can "see".

GVSC and industry partners, Peraton Labs and Noregon, have developed a data-bus agnostic, logically decoupled method of providing the assurance and verification of those vehicular microelectronics systems. The system utilizes radio frequency (RF) side channel analysis, a data exfiltration and exploitation modality, that has historically been an offensive cybersecurity capability, providing near-real time drop-in solutions for assuring ECUs [1].

2. BACKGROUND

The U.S. Army's weapon systems, the industrial controls used to manufacture them, and the associated supply chains remain vulnerable to compromise by adversarial offensive capabilities. These supply chains often lack robust controls at all points, both foreign and domestic. The United States is amid a security environment of unprecedented complexity, shaped by re-emerging nationalism, religious radicalism, uncertainty, and volatility [2].

Anti-competitive foreign trade practices are continually challenging U.S. strategic and critical microelectronics manufacturers. Damaging practices include nation-state sponsored dumping [3], public subsidies, and intellectual property (IP) theft. These have potential to compromise the commercial product integrity and economic security of domestic United States Department of Defense (DoD) suppliers. In numerous instances, the sole remaining domestic producer of materials critical to the DoD are on the verge of closing their U.S. factories. As a result, these U.S based producers often import lower cost materials from the same foreign producer country forcing them out of domestic production, thus further displacing overall domestic electronics production capabilities [4].

Current microelectronics are developed and manufactured at various foundries through the Anti-Tamper Executive Agent's Trusted Foundry program. However, this only provides protection at the manufacturing stage of the U.S. Army's supply chain. Numerous opportunities between the manufacturing and delivery/integration stages exist for malicious entities to add additional capabilities or perform alterations to vehicular microelectronics. Given the currently unsecure nature of vehicular data-bus networks, trust in the microelectronics in those networks is of paramount importance to achieve. One of the methods identified to achieve assurance and verification of vehicular microelectronics systems was the utilization of side-channel RF analysis technologies.

3. RADIO FREQUENCY SIDE-CHANNEL, A SHORT DIVE

Individual microelectronic systems emit an "unintended" electromagnetic emission on the radio frequency (RF) spectrum. These emissions are generated due to the local clock oscillator on a microelectronic system that generates the frequencies for logic [5]. The logic execution running on microelectronic systems cause fluctuations in these RF emissions.

To achieve the detection of these emissions in a real-world environment, frequency band scanning, a process of defining transmissions across a range of frequency bands, must be performed to quantify the RF device emanations and background noise for operations of the device.

4. SYSTEM ARCHITECTURE

The system architecture of the Assurance and Verification of Vehicular Microelectronic Systems (AV2MS) RF side-channel assurance technology contains two main components that enable detection of anomalous behavior of the microelectronic devices under test: Hardware and Algorithms.

4.1. HARDWARE

To read in RF emissions data from vehicular ECUs, various antenna types may be used depending on integration challenges.

Near-field antennas were utilized by GVSC to read RF emissions of vehicular microelectronic devices. The near-field antenna is physically air-gapped from, but placed close to, the microelectronic device under test. This antenna will pick up a wide range of emission frequencies, at high fidelity, in the RF spectrum.

A Rogowski Coil, shown in **Figure 1**, is the second method utilized by GVSC to read RF emissions from vehicular microelectronic devices. However, unlike the near-field antennae, the electrical power cables of the microelectronic device under test are run through the Rogowski Coil. The Rogowski Coil measures the RF emissions generated by the alternating current from these wires.

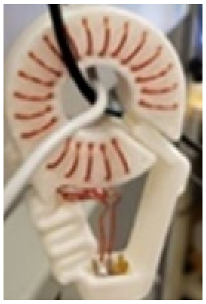

Figure 1: Rogowski Coil

Both near-field antennas and Rogowski Coils served as useful components for reading the unintended RF emissions from vehicular ECUs, therefore serving as a valuable sensor for evaluating cyber security and supply chain protection.

In addition to RF emissions, a vehicle data bus recorder collects in-vehicle network traffic to determine the current state of the vehicle, such as moving or stationary, and manual or autonomous mode. Obtaining this vehicle data is it critical to the system architecture of our use case.

4.2. ALGORITHMS

Machine learning (ML) algorithms serve as the key component for determining if a vehicular ECU is acting normally or maliciously. Machine Learning concepts are used to both train the system and monitor for anomalies.

4.2.1 TRAINING

Supervised Machine Learning trains the system to establish a functional baseline of the device under test. First, features are derived from the Fast Fourier Transform (FFT) of the RF signals [6]. These features are stored in a vector, later used for classifying the various functional modes of the ECUs.

Leveraging the Density-Based Spatial Clustering (DBSCAN) clustering algorithm (see **Figure 2**), these features are given artificial labels (modes). The DBSCAN algorithm groups and labels RF emission data based on high density clusters, while low density clusters are considered outliers.

These emission clusters are displayed in three-dimensional space using a Principal Component Analysis (PCA) plot. The PCA plots create visualizations that enable the user to clearly see the different clusters (functional modes) of the device under test, enabling human calibration of the system for additional detection accuracy.

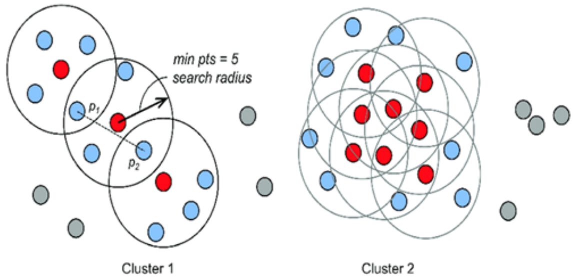

Figure 2: DBSCAN Clustering Algorithm [7]

During monitoring and detection, if an unknown mode is detected, the system uses Support Vector Machines (SVM) to calculate the probability that the unknown mode was misclassified. Data points that are classified as unknown after performing these calculations are considered anomalies [6]. Otherwise, the data point will be given the correct label.

4.2.2 DETECTION

After the system is trained, the detection algorithms are used to monitor the device under test for anomalies, or deviations from the trained datasets. The three concepts used are N-grams, Non-deterministic Finite-State Automata (NFA) and Statistical Detectors.

N-grams enable comparison of labeled data gathered from the RF emission and vehicle data of the microelectronic system. N-grams are a sequence, or pattern, of “n” elements within a given sequence of data [6]. Ultimately, N-grams monitor the labels to determine state changes from specific patterns, indicating if an anomaly is detected or not.

NFA is another method for determining if a device under test is functioning properly. NFA is a form of state machine that shows all possible paths, or decisions, a system could make, as seen in **Figure 3**. The system will create a state machine based off the pattern of RF emissions labels inferred by the training data [6]. Afterwards, the system will monitor the device’s states and paths, and if there is a deviation from trained data, then an anomaly is detected and subsequently flagged.

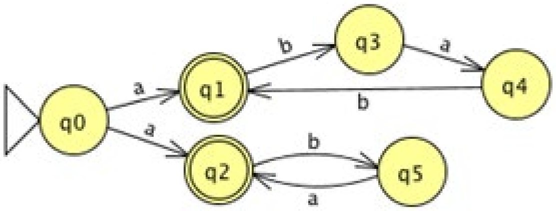

Figure 3: Non-Deterministic Finite-State Automata Example [8]

Lastly, Statistical Detectors rely upon the distribution properties of the training data (labels). As previously mentioned, the training data is stored in vectors, where its dimensions correspond to labels [6]. If the statistical distribution of the labels significantly differs from the current device label value, an anomaly has occurred.

The training and detection algorithms serve as critical components for the AV2MS system architecture. Utilizing multiple different Machine Learning methods, the technology provides vehicle platform owners with a high level of confidence in their microelectronic systems cyber posture, therefore advancing the state-of-the-art of vehicular cyber security.

5. Performance

5.1. Tests and Calibration

This RF side-channel assurance technology relies upon calibration to the system and operational environment that it is assuring. Due to numerous microelectronics emitting RF during operation, frequency band scanning must be performed to quantify the RF device emanations and background noise for operations of the device under test. After thorough testing, it was determined for the subject heavy vehicle platform, that the range for which these datapoints must be measured in is between 0 to 3 gigahertz to establish detection thresholds of the devices under test. This detection range may vary depending on the platform.

In the demonstration setup, the devices to assure were commercial, off-the-shelf (COTS) ECUs, integrated into a heavy vehicle platform, to serve as the operational RF environment to establish the detection thresholds.

In addition to RF emissions, vehicular data-bus messages were captured for the test, as they provided another layer of information to qualify detected ECU activity. With further detection threshold training, more precise antenna placement, and more access to information on the devices under test, the solution can provide higher fidelity of assurance.

To determine the AV2MS technology efficacy, the following test cases were designed to ensure that the system could quantify its operational RF environment, develop appropriate detection thresholds, and qualify the device emanation states from the ECUs. All test cases were conducted during a static demonstration on a ground vehicle platform.

1. Nominal Operation – This test case did not evaluate an attack, but rather was a test to ensure that the Assurance technology operated in accordance to system design.
2. Device State Changes – This test case evaluated an attack that exhibits a RF state change within the device under test. Evaluations were completed for comparison between nominal states, and malicious states of the ECUs. This test case showcased actions that could occur on a vehicular ECU that would not be detectable by ordinary intrusion detection and prevention system (IDPS) technologies.
3. Illicit Devices – This test case explored the detection of a separate, unconnected RF-emitting device within the vehicle platform. Here, a broad spectrum of detection capabilities was proven, as supply chain intrusions may result in illicit additional hardware being installed onto the vehicle platform.
4. Distributed Denial of Service (DDOS) – This test case explored a unique variation of state change. A DDOS may negatively impact the ability for a data-bus connected system to operate. However, due to the unique decoupled nature of the AV2MS RF side channel technology, the state changes occurring during a DDOS were detectable.

5.2. Results

In the principal component analysis (PCA) plot, shown in **Figure 4**, showcases one such example detailing the discrete clusters of emanation states in a representative test of the AV2MS RF side channel technologies, correlating to actions of the device (individually colored clusters), and the state transition changes (black points).

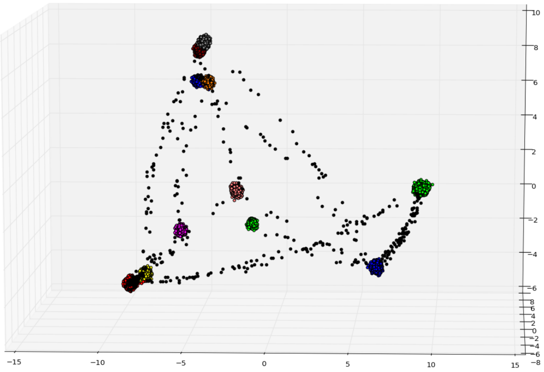

Figure 4: Principal Component Analysis Plot Result [6]

For evaluation, target thresholds for detection were set to require greater than 95% true positive rates, with false positive and false negative rates below 5% cumulatively. These criteria were applied to measure correctly identified malicious ECU states. The AV2MS RF side channel technology successfully demonstrated the prior four test cases, meeting a 95% true positive detection rate.

6. CONCLUSION

Supply chain cyber exploitation remains a highly attractive target to our adversaries. Significant vulnerabilities remain throughout the entire supply chain right up until vehicle installation and operation. Prior state-of-the-art technologies for detection of anomalous behavior in microelectronics systems have exploitable capability gaps. The AV2MS RF side channel technology demonstrates a novel, platform-agnostic system for edge-located assurance of vehicle electronic control unit (ECU) integrity. Utilization of RF side channel and machine learning techniques allow device states to be detected, quantified, and subsequently qualified in an emissions-heavy environment, providing a vector of assurance to augment vehicular platform supply chain controls. As such, assured vehicular platforms result in continued operation and operational availability, and improved cybersecurity.

7. REFERENCES

[1] D. Das and S. Sen, "Electromagnetic and Power Side-Channel Analysis: Advanced Attacks and Low-Overhead Generic Countermeasures through White-Box Approach," Cryptography, vol. 4, no. 4, p. 30, Oct. 2020. Accessed: Mar. 16, 2022. [Online]. Available: https://doi.org/10.3390/cryptography4040030

[2] The White House, “Interim National Security Strategic Guidance – March 2021”, The White House, Washington D.C., 2021

[3] A. Barone, Investopedia, 2020. [Online]. Available: https://www.investopedia.com/terms/d/dumping.asp. [Accessed: 08-Mar-2022]

[4] Department of Defense (DoD) Industrial Policy, “Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States.”

[5] Acharya, S., 2015. Detection and Recognition of R/F Devices Based on Their Unintended Electromagnetic Emissions using Stochastic and Computational Intelligence Methods. Ph.D. Missouri University of Science and Technology.”

[6] S. Alexander, H. Agrawal, R. Chen, J. K. Hollingsworth, C. Hung, R. Izmailov, J. Koshy, J. Liberti, C. Mesterharm, J. Morman, T. Panagos, M. Pucci, I. Sebuktekin, and S. Tsang, “Casper: An efficient approach to detect anomalous

code execution from unintended electronic device emissions," Cyber Sensing 2018, 2018.

[7] D. A. Bonneau, "The Implications of M3C2 Projection Diameter on 3D Semi-Automated Rockfall Extraction from Sequential Terrestrial Laser Scanning Point Clouds - Scientific Figure on ResearchGate." Available: https://www.researchgate.net/figure/The-DBSCAN-algorithm-and-two-generated-clusters-There-are-three-types-of-points-as_fig2_342082665 [Accessed: 9-Mar-2022]

[8] R. M. Kline, "5. Nondeterministic Finite Automata." [Online]. Available: https://www.cs.wcupa.edu/rkline/fcs/nfas.html. [Accessed: 15-Mar-2022].