International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Emerging Security Risks in Automotive System-on-Chips (SoCs): A Comprehensive Review

Sujan Hiregundagal Gopal Rao

Submitted:08/11/2022 **Accepted:**14/12/2022 **Published:25/12/2022**

Abstract: The transformation of modern vehicles into highly connected and software-driven systems has positioned System-on-Chips (SoCs) as a central element of automotive innovation. Automotive SoCs combine heterogeneous processing cores, accelerators, memory subsystems, and communication interfaces to support safety-critical functionalities such as Advanced Driver Assistance Systems (ADAS), autonomous driving, infotainment, and vehicle-to-everything (V2X) communication. While this high level of integration improves performance and cost efficiency, it also gives rise to new and increasingly complex security challenges. This paper presents a comprehensive review of emerging security risks affecting automotive SoCs, encompassing hardware-based attacks, software and firmware vulnerabilities, network-oriented exploits, and systemic risks associated with over-the-air updates and AI-driven workloads. By synthesizing recent academic and industrial research, the paper identifies dominant attack vectors, shortcomings of existing protection mechanisms, and open challenges that remain unresolved. The goal is to provide both researchers and practitioners with a structured perspective on the evolving threat landscape and to outline directions for security-aware SoC design.

Keywords: *Automotive cybersecurity, System-on-Chip (SoC), hardware security, connected vehicles, ADAS, secure automotive electronics*

1. Introduction

The automotive sector has evolved from predominantly mechanical systems into sophisticated cyber-physical platforms driven by electronics and software. Modern vehicles integrate a large number of electronic control units (ECUs) interconnected through in-vehicle networks, with many functions increasingly consolidated onto high-performance automotive SoCs. These SoCs serve as centralized computing platforms supporting perception, control, decision-making, and connectivity, particularly in autonomous and software-defined vehicles.

Although functional consolidation improves scalability and computational efficiency, it also concentrates security risks. A vulnerability within an automotive SoC can potentially affect multiple vehicle subsystems simultaneously. Moreover, automotive environments impose strict real-time and safety constraints, which limit the direct adoption of conventional IT security techniques. Consequently, identifying and understanding emerging SoC-level security risks has become a critical concern for both academia and industry [1].

2. Automotive SoC Architecture and Security Context

Automotive SoCs typically integrate general-purpose processors, real-time microcontroller cores, graphics processors, AI accelerators, memory subsystems, and diverse communication interfaces onto a single chip. These components collectively support workloads ranging from hard real-time control tasks to compute-intensive data processing.

Figure 1 presents a high-level view of an automotive SoC and its interaction with external vehicle domains.

sujangopalrao@gmail.com
Independent Researcher, USA

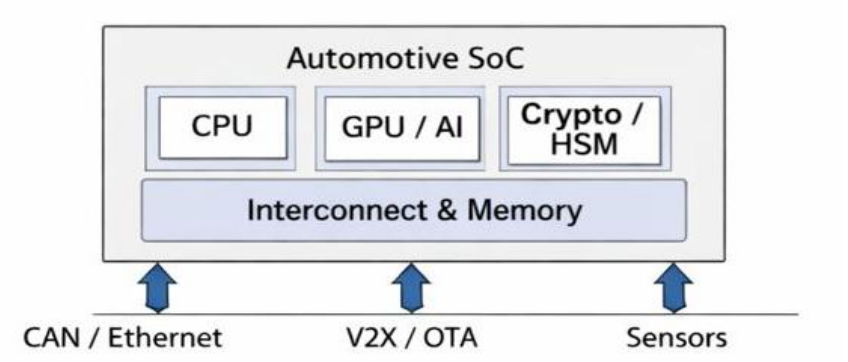

Figure 1. High-Level Automotive SoC Architecture and Attack Surface

The architectural heterogeneity and tight coupling between components significantly increase the attack surface, particularly at interfaces separating safety-critical and non-safety domains.

3. Literature Review

Recent studies increasingly emphasize the security implications of automotive SoC integration from both academic and industrial perspectives. Early work in automotive cybersecurity focused primarily on vulnerabilities in in-vehicle communication protocols, especially the absence of authentication and encryption in CAN networks [2]. As SoCs assumed a more central role, research attention expanded toward vulnerabilities spanning both hardware and software layers.

Several investigations have analyzed firmware integrity and boot-chain security, demonstrating that weaknesses in secure boot processes or cryptographic key management can compromise the entire trust model of an SoC [3]. Other studies have examined side-channel and fault-injection attacks on automotive-grade hardware, revealing that cost and power constraints often limit the effectiveness of traditional countermeasures [4].

More recent contributions explore real-time monitoring and intrusion detection mechanisms implemented at the SoC level. Machine learning–based approaches have been proposed to detect anomalies in automotive Ethernet and SOME/IP traffic, enabling the identification of denial-of-service and spoofing attacks [5]. In parallel, large-scale vulnerability assessments aligned with AUTOSAR architectures have highlighted recurring issues such as weak access control, insecure inter-process communication, and delayed security updates [6].

Table 1. Summary of Representative Literature on Automotive SoC Security

Author / Year	Focus Area	Methodology	Key Findings
Checkoway et al., 2011	In-vehicle network attacks	Experimental vehicle attacks	Demonstrated remote exploitation paths
Sanwald et al., 2020	Secure boot	Hardware analysis	Key mismanagement weakens root of trust
Wolf et al., 2021	Automotive hardware security	Survey	Need for SoC-level isolation

4. Emerging Security Risks in Automotive SoCs

4.1 Hardware-Level Threats

Hardware-based attacks are particularly critical because of their persistence and low detectability. Supply-chain attacks may introduce malicious modifications during the design or fabrication stages [7]. Side-channel attacks exploiting power consumption, timing variations, or electromagnetic emissions have demonstrated the feasibility of extracting cryptographic secrets from automotive SoCs under realistic conditions [8]. Fault-injection techniques further allow attackers to bypass security checks by deliberately inducing transient hardware errors.

4.2 Software and Firmware Vulnerabilities

Automotive SoCs rely on complex firmware stacks that include bootloaders, hypervisors, and real-time operating systems. Vulnerabilities within these layers can enable privilege escalation or arbitrary

code execution. While over-the-air updates are essential for maintenance and feature deployment, they also create additional attack vectors if authentication, integrity checks, or rollback protections are inadequately implemented [9].

4.3 Network and Communication-Based Attacks

The adoption of automotive Ethernet and V2X communication increases exposure to remote threats. Legacy protocols such as CAN and SOME/IP lack intrinsic security features, enabling message injection, replay, and denial-of-service attacks [10].

Figure 2 illustrates common attack paths targeting automotive SoCs through external interfaces.

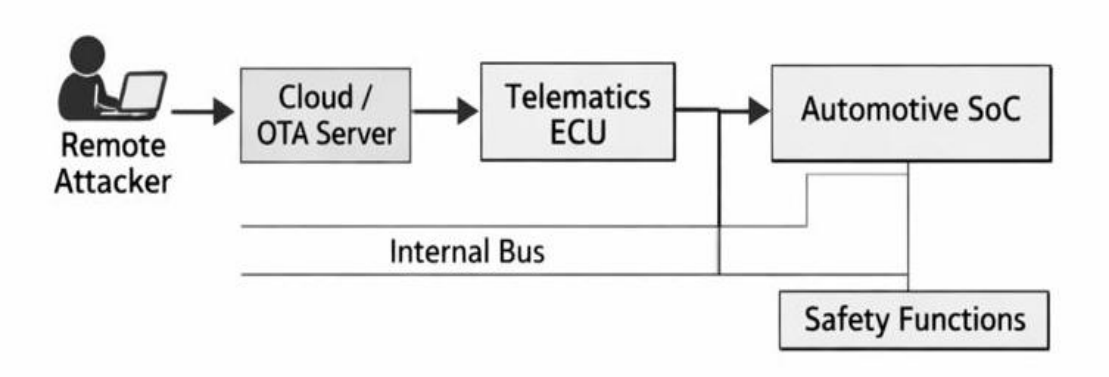

Figure 2. Typical Attack Paths Targeting Automotive SoCs

4.4 AI and Data-Driven Risks

AI accelerators embedded within automotive SoCs support perception and decision-making functions but also introduce novel security risks. Adversarial inputs and model manipulation can degrade system reliability and compromise safety, particularly in autonomous driving contexts [11].

5. Comparative Analysis of Threats and Impacts

Security threats targeting automotive SoCs differ in terms of attack complexity, entry points, and potential impact on vehicle operation. Hardware-level attacks, although technically demanding, can lead to long-term and stealthy compromises that undermine the foundational trust of the system. Firmware and network-based attacks are typically easier to execute remotely and can disrupt multiple vehicle functions due to the centralized nature of SoCs. AI-related threats, while still emerging, pose significant safety concerns by subtly influencing perception or decision-making processes without triggering conventional fault detection. A clear understanding of these distinctions is essential for prioritizing mitigation strategies and allocating security resources effectively.

Table 2. Automotive SoC Threats and Potential Impacts

Threat Category	Example Attacks	Potential Impact
Hardware attacks	Side-channel, fault injection	Key leakage, bypassed security
Firmware exploits	Insecure boot, OTA abuse	Persistent compromise
Network attacks	CAN injection, Ethernet DoS	Loss of control, service disruption
AI attacks	Adversarial inputs	Unsafe vehicle behavior

6. Mitigation Strategies and Design Considerations

Mitigating automotive SoC security risks requires a layered defense strategy spanning both hardware and software. Hardware roots of trust, secure boot mechanisms, and isolated security modules establish a foundation for system integrity. At the software level, strong partitioning, least-privilege access control, and continuous monitoring are critical. Intrusion detection systems embedded at the SoC level can provide real-time visibility into abnormal behavior and emerging threats [12].

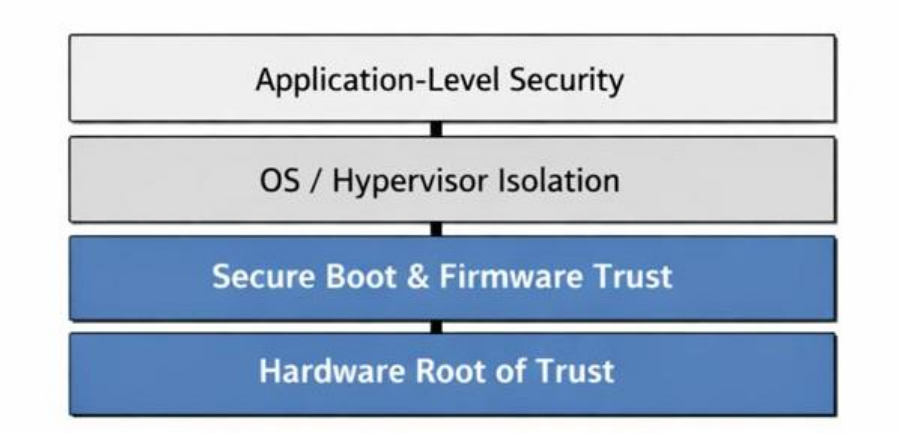

Figure 3. Layered Security Approach for Automotive SoCs

7. Open Challenges and Future Research Directions

Despite ongoing progress, automotive SoC security continues to face fundamental challenges driven by architectural heterogeneity, strict real-time constraints, and long operational lifetimes.

7.1 Open Technical Challenges

- **Heterogeneous SoC architectures:** The integration of real-time cores, high-performance CPUs, GPUs, and AI accelerators over shared interconnects complicates spatial and temporal isolation, particularly in the presence of shared memory, caches, and DMA mechanisms.
- **Real-time security trade-offs:** Cryptographic processing, secure context switching, and runtime monitoring introduce latency and execution-time variability, making it difficult to preserve worst-case execution time guarantees.
- **Limited hardware-level observability:** Hardware attacks such as side-channel analysis and fault injection operate below software visibility, while automotive-grade on-chip detection mechanisms remain immature.
- **Long-term resilience:** Automotive SoCs must remain secure over extended lifetimes, requiring cryptographic agility, secure key renewal, and evolution of hardware-rooted trust mechanisms.

7.2 Future Research Directions

- **Safety–security co-design:** Early integration of cybersecurity requirements with functional safety analysis to capture cascading effects.
- **Adaptive and reconfigurable security:** Programmable security components that allow defenses to evolve post-deployment.
- **Certifiable intelligent security mechanisms:** Explainable and verifiable AI-based intrusion detection suitable for automotive certification.
- **Cross-layer modeling and verification:** Unified approaches that analyze security properties across hardware, firmware, operating systems, and applications.

Addressing these issues demands coordinated research across semiconductor design, real-time systems, and automotive cybersecurity.

Conclusion

Automotive SoCs have become a foundational element of modern vehicles, enabling advanced functionality while introducing complex security challenges. This review examined emerging threats across hardware, software, network, and AI domains and emphasized the need for holistic, SoC-centric security strategies. Addressing these challenges is essential to ensure the safety, reliability, and trustworthiness of next-generation automotive systems.

References

[1] Wolf, M., Weimerskirch, A., & Paar, C. (2021). Security in automotive bus systems. *Proceedings of the IEEE*, 109(3), 343–356.

[2] Checkoway, S., et al. (2011). Comprehensive experimental analyses of automotive attack surfaces. *USENIX Security Symposium*, 77–92.

[3] Sanwald, T., et al. (2020). Secure boot mechanisms in automotive ECUs. *IEEE Embedded Systems Letters*, 12(2), 45–48.
[4] Eisenbarth, T., et al. (2019). On the power of power analysis in embedded systems. *IEEE Transactions on Computers*, 68(1), 3–16.
[5] Tehranipoor, M., & Wang, C. (2017). *Introduction to hardware security and trust*. Springer.
[6] Mangard, S., Oswald, E., & Popp, T. (2007). *Power analysis attacks*. Springer.
[7] Nilsson, D., Larson, U., & Jonsson, E. (2018). Securing vehicle OTA updates. *Computer*, 51(7), 38–47.
[8] Hoppe, T., Kiltz, S., & Dittmann, J. (2011). Security threats to automotive CAN networks. *Automotive Safety & Security*, 235–248.
[9] Eykholt, K., et al. (2018). Robust physical-world attacks on machine learning models. *CVPR*, 1625–1634.
[10] Studnia, I., et al. (2020). Survey on intrusion detection in automotive networks. *IEEE Communications Surveys & Tutorials*, 22(4), 2474–2509.
[11] ISO/SAE. (2021). ISO/SAE 21434: Road vehicles — Cybersecurity engineering.
[12] Sommer, R., & Paxson, V. (2010). Outside the closed world: IDS challenges. *IEEE Symposium on Security and Privacy*, 305–316.
[13] Chattopadhyay, A., et al. (2022). Security-aware SoC design for automotive systems. *ACM TODAES*, 27(4), 1–29.