International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 4, pp 34-38, April-2024

https://doi.org/10.47001/IRJIET/2024.804004

Secure Over-the-Air (OTA) Update Mechanisms for ADAS

Alex Mathew

Department of Cybersecurity, Bethany College, USA

Abstract **- This research aims to develop robust, resilient, and user-friendly over-the-air (OTA) software update mechanisms for advanced driver assistance systems (ADAS) in modern vehicles. The study conducts a comprehensive review on existing OTA update approaches, identifies security threats and vulnerabilities, and proposes an algorithm that incorporates cryptographic techniques, secure authentication, firmware validation, and rollback protection. The methodology utilized in this study involves secure package generation, distribution, installation, and monitoring, as well as adhering to automotive cybersecurity standards, such as ISO/SAE 21434 and UNECE WP.29. Extensive evaluation of OTA systems is important as it helps to assess their resilience against adversarial attacks, ensures regulatory compliance, and optimizes usability through user studies. The results demonstrate successful execution of secure OTA update mechanisms, preventing risks, fostering reliability and safety of ADAS software updates. The case studies highlight real-world deployments, best practices, and the effectiveness of the developed solution in improving automotive cybersecurity and functional safety.**

Keywords: User-friendly over-the-air, advanced driver assistance systems, modern vehicles, safety, software updates.

I. INTRODUCTION

In the past decade, advanced driver assistance systems have become an important part of modern vehicles due to their ability to enhance safety and convenience for drivers. However, the software that drives systems needs frequent updates to address security lapses, add new features, and enhance functionality. With ADA systems requiring frequent software updates, the OTA software updates have become extremely popular in modern vehicles due to their ability to provide convenient and efficient solutions. However, OTA software updates are risk introducing significant security risks into the ADA systems if they are not implemented properly. The update process can be tampered or exploited for vulnerabilities by malicious actors, which ends up compromising the integrity and safety of ADAS systems. This research study seeks to develop robust, resilient, and user-friendly OTA update mechanisms that address security concerns and enhance the cybersecurity and functional safety of ADAS in modern vehicles.

II. PROPOSED METHODOLOGY BLOCK DIAGRAM

The methodology for this research paper begins with a comprehensive review of existing OTA update mechanisms, which are employed in ADAS systems. This comprehensive review provides a baseline comprehension of the current state of OTA updates for ADAS. After the comprehensive review, the security threat landscape will be explored to help identify potential vulnerabilities, attack vectors, and risks that are linked to OTA update mechanisms. This step lays bare the critical security considerations that need to be addressed.

The research then explores how cryptographic protocols and techniques can be utilized to ensure confidentiality, integrity, and authenticity of OTA update packages that are transmitted OTA. This includes examining digital signatures, message authentication codes (MACs), and secure hash algorithms. This will be followed by developing robust authentication and authorization mechanisms, which can help verify the identities and permissions of both the update server and the receiving ADAS components prior to the start of the update process. The goal of developing these mechanisms is to mitigate further unauthorized updates and prevent the risk of malicious actors exploiting the update mechanism.

Secure boot mechanisms and firmware validation processes are implemented to ensure that only trusted and verified software updates are installed on ADAS components. This step involves verifying the integrity and authenticity of firmware images, enforcing secure boot policies, and detecting and preventing unauthorized modifications or rollback attacks.

This is followed by an evaluation of the resilience of the proposed mechanisms against adversarial attacks, such as buffer overflows and code injection is evaluated. Conducting these evaluations will help to develop countermeasures and intrusion detection techniques so as to help mitigate breaches. Next, an assessment on usability and user experience will be conducted to ensure that security measures do not cause a lot of inconvenience to users through studies and feedback sessions. The methodology will also seek to ensure the proposed and adopted security mechanisms comply with

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 8, Issue 4, pp 34-38, April-2024
https://doi.org/10.47001/IRJIET/2024.804004

automotive cybersecurity standards, such as ISO/SAE 21434, UNECE WP.29, and ISO 26262 for functional safety is ensured. Lastly, case studies will be introduced to indicate the success of past real-world deployments, reveal the lessons learned, and propose the best practices for secure, reliable OTA updates in ADAS systems.

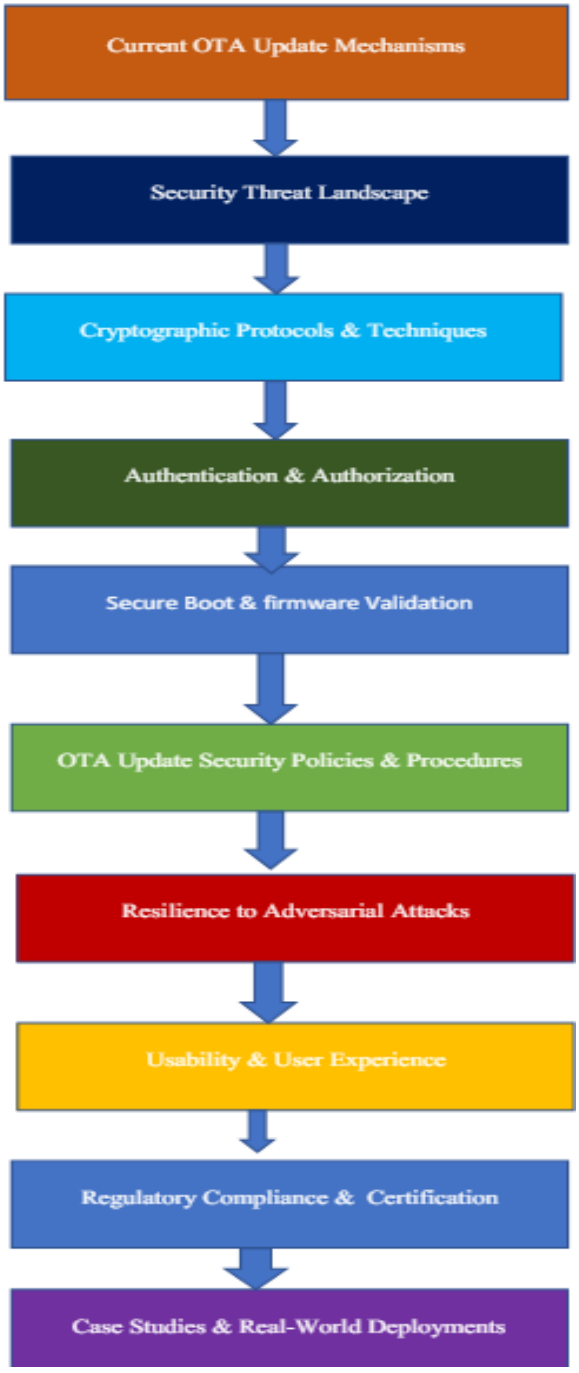

Figure 1: Proposed Methodology Block Diagram

III. ALGORITHM

This research seeks to develop a robust, resilient, and user-friendly software update mechanisms that can be used to enhance the security, reliability, and safety of ADA systems in modern vehicles. Achieving this objective will require deploying an algorithm that can help to securely manage the entire OTA update lifecycle, from package generation and distribution to installation and verification. The proposed algorithm begins with generating an updated software package using the authorized update server. The updated package comprises of a new software version, metadata, consisting of version numbers and compatibility information, as well as a digital signature. The digital signature is developed using secure cryptographic algorithm, such as an elliptic curve digital signature algorithm (ECDSA) and the server's private keys (Shankar, et al. 2). Using a combination of the tools to develop the algorithm will ensure the authenticity and integrity of the update package.

Next, the update package needs to be securely distributed to the target ADAS components, such as sensors, control units, and infotainment systems using a secure communication channel, such as a datagram transport layer security (DTLS) (Novikov). This intervention will ensure the confidentiality and integrity of the update package during transmission.

After receiving the update package, the ADAS component will verify the authenticity of the update server by validating its digital certificate and checking the revocation status. However, mutual authentication will need to be conducted to help establish trust between the server and the ADAS component. This is followed by a package integrity reverification to ensure that the update package has not been tampered with during transmission (Danahata).

Prior to installing the update, a secure bot process will be need to be performed by the ADAS component to validate the new software version against a trusted reference. Secure boot and firmware validation ensure that only authorized and verified updates are installed and rollback attacks and unauthorized modifications are mitigated.

If the update package passes all security checks, the ADAS component will go ahead to install the new software version. ADAS component will need, after installation, to perform integrity checks and functional tests to verify if it is a successful update.

The entire update process is monitored and logged for auditing and forensic purposes, with security events, such as failed authentication attempts or integrity verification failures, being recorded and analyzed for potential threats or anomalies. This algorithm adheres to industry standards and best practices, such as ISO/SAE 21434, UNECE WP.29, and ISO 26262, which ensure that players in the sector comply regulatory requirements and certification guidelines for cybersecurity and functional safety in automotive systems (Li et al. 2).

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 8, Issue 4, pp 34-38, April-2024
https://doi.org/10.47001/IRJIET/2024.804004

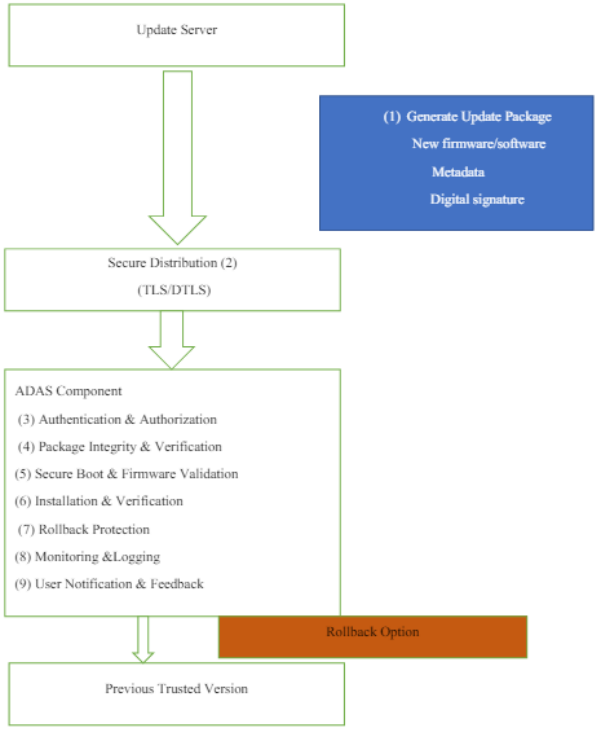

Figure 2: Algorithm for the ADA systems

IV. FLOW CHART

The flowchart starts with the initiation of the OTA update process, followed by the authentication of the update server to establish trust and ensure that the update package is coming from an authorized source. If the authentication fails, the update is rejected, and the failure is logged and reported. If the server authentication is successful, the update package is verified for integrity using cryptographic techniques, such as digital signatures or secure hashes (Xu et al. 2). If the integrity check fails, the update is rejected, and the failure is logged and reported.

After the update package integrity has been verified, the new software version is validated against a trusted reference and secure boot mechanisms. If the validation becomes unsuccessful, the update is rejected, and the system can switch back to the preceding trusted version (Federal Student Aid). However, if the validation is successful, the update is installed on the ADAS component.

Once the installation in the ADAS component occurs, the system validates the successful update and notifies the user about the update status and user feedback is collected to enhance the usability and user experience of the update process (Nandavar et al. 342). Nevertheless, failure in the validation process will necessitate adoption of rollback protection mechanisms that can help the system revert to the previous trusted version of the software. Throughout the process, there is constant auditing and monitoring of the success and failure events to ensure they are successfully logged (Mehta et al. 648). This flowchart aligns with industry best practices and standards, such as ISO/SAE 21434 and UNECE WP.2, which outline the guidelines for cybersecurity and software update management in automotive systems.

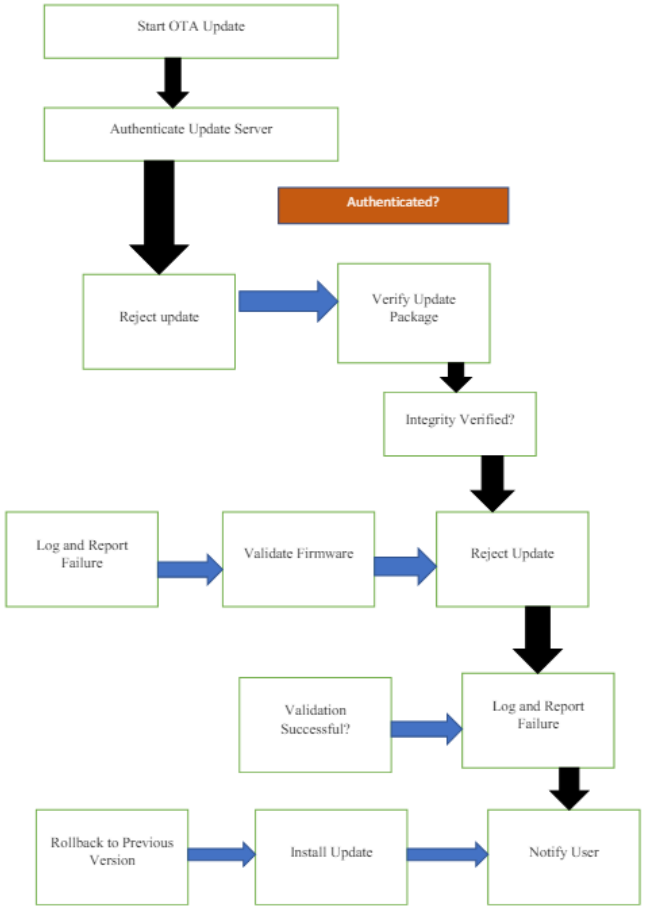

Figure 3: Flowchart for OTA Update

V. RESULTS AND DISCUSSIONS

The research study on "Secure OTA Update Mechanisms for ADAS" aims to develop and deploy robust, resilient, and user-friendly software update mechanisms that enhance the security, reliability, and safety of advanced driver assistance systems in modern vehicles. The results of this research can be analyzed based on the outlined methodology and research objectives.

The study conducted a comprehensive review of existing OTA update mechanisms that are utilized in ADAS systems, including their protocols, architectures, and technologies. The analysis helped to identify the strengths and weaknesses of current approaches and this paved the way to make improvements in security, reliability, and user-friendliness. The study results show that many existing OTA update mechanisms do not embrace the requisite robust security measures, which makes them increasingly vulnerable to

ISSN (online): 2581-3048
Volume 8, Issue 4, pp 34-38, April-2024
https://doi.org/10.47001/IRJIET/2024.804004

various cybersecurity attacks (Mahmood et al. 2: Safitra et al. 4).

An analysis on the security threat landscape of the OTA update mechanisms for ADAS highlighted the importance of addressing security risks to ensure the integrity and safety of ADAS systems as they are prone to critical attack vectors, such as interception, tampering, replay attacks, and unauthorized access to update servers or communication channels (Sheik et al. 18).

Research on cryptographic protocols and techniques, such as digital signatures, message authentication codes (MACs), and secure hash algorithms, showed that these tools are necessary in ensuring confidentiality, integrity, and authenticity of OTA update packages (Faster Capital). They mitigate unauthorized modifications and ensure the trustworthiness of updates.

The development and testing of the authentication and authorization mechanisms through mutual authentication, access controls, and role-based authorization policies revealed that those mechanisms play an influential role in preventing the risk of unauthorized updates and curtail malicious actors from exploiting the update mechanism (Şeker et al. 2: Fareed and Yassin 4). This, in turn, enhances the security of the ADAS system.

The implementation of secure boot mechanisms and firmware validation processes in the ADA systems revealed that there is a significant reduction in the risk of unauthorized modifications, rollback attacks, and the installation of compromised firmware. This aligns with the guidelines that are outlined in the UNECE WP.29 (4) regulations (SiBrain Technologies). The study results indicate that successful development and deployment of secure, robust, and user-friendly OTA update mechanisms for ADAS systems helps to address critical security, reliability, and safety requirements of modern vehicles.

VI. CONCLUSION

Modern vehicles increasingly rely on ADA systems that, unfortunately, need frequent software updates. OTA updates provide much more convenience but pose major risks if they are not implemented securely because malicious actors can exploit vulnerabilities in the update process. The research results indicate that incorporating cybersecurity solutions, such as firmware validation, cryptography, and secure authentication can enhance cybersecurity and functional safety of ADAS.

REFERENCES

[1] Danahata, Amos. "Package Verification Failed - Make It Stop!" XDA Forums, 14 Jan. 2022, xdaforums.com/t/package-verification-failed-make-it-stop.4388055/.

[2] Fareed, Mohammad, and Ali A. Yassin. "Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system." Bulletin of Electrical Engineering and Informatics, vol. 11, no. 4, 2022, pp. 2131-2141.

[3] Faster Capital. "Cryptography Based Security: Enhancing Message Authentication Codes." FasterCapital, 7 Mar. 2024, fastercapital.com/content/Cryptography-based-security--Enhancing-Message-Authentication-Codes.html.

[4] Federal Student Aid. "Verification, Updates, and Corrections." FSA Partner Connect, 28 Mar. 2021, fsapartners.ed.gov/knowledge-center/fsa-handbook/2022-2023/application-and-verification-guide/ch4-verification-updates-and-corrections.

[5] Li, Yufeng, et al. "Complying with ISO 26262 and ISO/SAE 21434: A Safety and Security Co-Analysis Method for Intelligent Connected Vehicle." Sensors, vol. 24, no. 6, 2024, p. 1848.

[6] Mahmood, Shahid, et al. "Systematic threat assessment and security testing of automotive over-the-air (OTA) updates." Vehicular Communications, vol. 35, 2022, p. 100468.

[7] Mehta, Aryan A., et al. "Securing the Future: A Comprehensive Review of Security Challenges and Solutions in Advanced Driver Assistance Systems." IEEE Access, vol. 12, 2024, pp. 643-678.

[8] Nandavar, Sonali, et al. "Exploring the factors influencing acquisition and learning experiences of cars fitted with advanced driver assistance systems (ADAS)." Transportation Research Part F: Traffic Psychology and Behaviour, vol. 94, 2023, pp. 341-352.

[9] Novikov, Ivan. "Streamline Your Online Security with DTLS: A Guide." Wallarm, 26 Feb. 2024, www.wallarm.com/what/what-is-datagram-transport-layer-security-dtls.

[10] Safitra, Muhammad F., et al. "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity." Sustainability, vol. 15, no. 18, 2023, p. 13369.

[11] Shankar, Gauri, et al. "Improved Multisignature Scheme for Authenticity of Digital Document in Digital Forensics Using Edward-Curve Digital Signature Algorithm." Security and Communication Networks, vol. 2023, 2023, pp. 1-18.

[12] Sheik, Al T., et al. "Securing Cloud-Assisted Connected and Autonomous Vehicles: An In-Depth

ISSN (online): 2581-3048
Volume 8, Issue 4, pp 34-38, April-2024
https://doi.org/10.47001/IRJIET/2024.804004

Threat Analysis and Risk Assessment." Sensors, vol. 24, no. 1, 2023, p. 241.

[13] SiBrain Technologies. "Exploring Secure Boot Mechanisms in Embedded Systems: Ensuring Firmware Integrity and Authenticity." LinkedIn, 10 Mar. 2024, www.linkedin.com/pulse/exploring-secure-boot-mechanisms-embedded-systems-ensuring-4pdlf.

[14] Xu, Dingjie, et al. "Integrity Authentication Based on Blockchain and Perceptual Hash for Remote-Sensing Imagery." Remote Sensing, vol. 15, no. 19, 2023, p. 4860.

[15] Şeker, Özlem, et al. "MARAS: Mutual Authentication and Role-Based Authorization Scheme for Lightweight Internet of Things Applications." Sensors, vol. 23, no. 12, 2023, p. 5674.

AUTHOR'S BIOGRAPHY

Dr. Alex Mathew
Associate Professor,
Cybersecurity & Data Science,
Bethany College, USA.

Citation of this Article:

Alex Mathew, "Secure Over-the-Air (OTA) Update Mechanisms for ADAS" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 4, pp 34-38, April 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.804004

****

