Conferences >2023 International Conference...

Systematic Review on the Recent Trends of Cybersecurity in Automobile Industry

Publisher: IEEE

Cite This

PDF

Chidera Prince Eze; Jerry Emmanuel; Christopher Iyanu-Oluwa Onietan; Itunuoluwa Isewon; Jelili Oyelade

All Authors

1

Abstract

Document Sections

- V.

  Conclusion

Authors
Figures
References
Citations
Keywords
Metrics

Abstract:

The increasing integration of technology in automobiles has raised industry concerns about cyber-security. This paper provides an overview of the most recent developments in automobile cyber-security practices, pointing out the most important areas of cyber security that need more research in the context of self-driving cars and the automobile industry. Considering the different communities of cybersecurity mapped out by previous researchers, we explored each of these communities with respect to automobiles. The community of cybersecurity is subjected to intrusion detection, cryptography, sensor networks, information hiding, intrusion detection, biometrics, authentication, usable security, and access control. From the systematic review done, we found out the bulk of security research in the automobile industry is geared towards intrusion detection. The use of chaos-based picture encryption, visual cryptography, biometric fingerprinting, keystroke dynamics, background subtraction, gait identification, provable security, provable data possession, block ciphers, differential power analysis, hardware trojans, physical unclonable functions, etc., although used in the industry, has yet to be explored with respect to the security of vehicles, their networks, and the automobile industry. The results show that some of the different communities of cybersecurity towards automobiles are still in their infancy with opportunities for novel work.

Published in: 2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)
Date of Conference: 05-07 April 2023
Date Added to IEEE *Xplore*: 22 May 2023
ISBN Information:
DOI: 10.1109/SEB-SDG57117.2023.10124561
Publisher: IEEE
Conference Location: Omu-Aran, Nigeria

I. Introduction

Since the beginning of the 20th century, advances in automotive technology and manufacturing have led to explosive expansion in the global car industry. It was believed that the twenty-first century would be the period in which individual automobile components would be able to communicate with one another and share resources inside the vehicle system [1]. The controller area network (CAN) was the impetus for this change. Protection of the in-vehicle network is meant when cybersecurity in the automotive sector is discussed [2]. Electronic control units (ECUs) are only one kind of device that hackers often target as entry points for their cyberattacks. According to Moller et al. [3], a consequence of this is that intrusion detection systems (IDS) have to be deployed as a component of cybersecurity measures in order to block these entry points into an in-vehicle network.

Sign in to Continue Reading
Authors
Figures
References
Citations
Keywords
Metrics

More Like This

Home Care Automation: Market Research, Industry Analysis, and Security Assessment

2023 International Conference On Cyber Management And Engineering (CyMaEn)

Published: 2023

A New Trend in Cryptographic Information Security for Industry 5.0: A Systematic Review

IEEE Access