Title: ***STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System***

Author Names: Popy Das ,Md. RashidAlAsif , Sohely Jahan Rahamatullah Khondoker

Abstract: In modern automobiles, the infotainment system is crucial for enhancing driver and passenger capabilities, offering advanced features such as music, navigation, communication, and entertainment. Leveraging Wi-Fi, cellular networks, NFC, and Bluetooth, the system ensures continuous internet connectivity, providing seamless access to information. However, the increasing complexity of IT connectivity in vehicles raises significant cybersecurity concerns, including potential data breaches and exposure of sensitive information. To enhance security in infotainment systems, this study applied component-level threat modeling to a proposed infotainment system using the Microsoft STRIDE model. This approach illustrates potential component-level security issues impacting privacy and security concerns. The study also assessed these impacts using SAHARA and DREAD risk assessment methodologies. The threat modeling process identified 34 potential security threats, each accompanied by detailed information. Moreover, a comparative analysis is performed to compute risk values for prioritizing treatment, followed by recommending mitigation strategies for each identified threat. These identified threats and associated risks require careful consideration to prevent potential cyberattacks before deploying the infotainment system in automotive vehicles.

Keywords: cybersecurity; infotainment; threat modeling; risk assessment; threat mitigation

https://doi.org/10.3390/vehicles6030054

https://www.mdpi.com/2624-8921/6/3/54