

Highway to Hack - Security gaps in ETSI ITS standards

R. Gesteira Miñarro; T. Yoshizawa; R. Palacios Hielscher; G. López López

Abstract-

Vehicle-to-Everything (V2X) communication technologies are revolutionizing transportation by enabling real-time information exchange among vehicles, infrastructure, pedestrians, and networks. While these technologies offer significant benefits in terms of road safety, traffic efficiency, and support for autonomous driving, they also introduce critical security and privacy risks due to their decentralized and dynamic nature. In this paper, we perform an analysis of the ETSI Intelligent Transport System (ITS) standards, specifications and reports to identify vulnerabilities that could be exploited to cause cyber–physical damages. We focus particularly on Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM) in the ETSI ITS standard, and pseudonym ID mechanisms. We identified several security issues, including vulnerabilities that lead to replay attacks, identity-based attacks such as spoofing and Sybil attacks, as well as grayhole attacks. We present attack scenarios where the issues found can be leveraged to compromise road safety, and quantify their potential impact through simulations using Eclipse SUMO. These scenarios might be relevant during a transition period where V2X-enabled vehicles coexist with legacy vehicles. Furthermore, we propose mitigations to address the identified issues. Our findings highlight the need for stronger security measures in V2X systems to ensure both safety and security in future intelligent transportation systems.

Index Terms- Cooperative awareness; Vehicle-to-everything; Replay attack; Pseudonym; Simulation; Cybersecurity

Due to copyright restriction we cannot distribute this content on the web. However, clicking on the next link, authors will be able to distribute to you the full version of the paper:

[Request full paper to the authors](#)

If your institution has an electronic subscription to Computer Standards & Interfaces, you can download the paper from the journal website:

[Access to the Journal website](#)

Citation:

Gesteira-Miñarro, R.; Yoshizawa, T.; Palacios, R.; López, G. "Highway to Hack -

Security gaps in ETSI ITS standards", Computer Standards & Interfaces, vol.97, pp.104133-1-104133-10, April, 2026.