Workgroup: IPWAVE Working Group
Internet-Draft:
draft-jeong-ipwave-security-privacy-06
Published: 25 July 2022
Intended Status: Standards Track
Expires: 26 January 2023
Authors: J. Jeong, Ed. Sungkyunkwan University
Y. Shen Sungkyunkwan University
H. Jung Sungkyunkwan University
J. Park ETRI
T. Oh Rochester Institute of Technology

Basic Support for Security and Privacy in IP-Based Vehicular Networks

Abstract

This document describes possible attacks of security and privacy in IP Wireless Access in Vehicular Environments (IPWAVE). It also proposes countermeasures for those attacks.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 26 January 2023.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Vehicular networking has become popular by the enhancement of Intelligent Transportation Systems (ITS) [ISO-ITS-IPv6]. The vehicular networking can work based on Dedicated Short-Range Communications (DSRC) [DSRC]. This DSRC is realized by the IEEE Wireless Access in Vehicular Environments (WAVE) [WAVE-1609.0]. Especially, IEEE 802.11-OCB (Outside the Context of Basic Support Set) [IEEE-802.11-OCB] provides the Media Access Control (MAC) for vehicles in vehicular networks. IP-based vehicular networking can be supported with IPv6 over IEEE 802.11-OCB [RFC8691], which defines the IPv6 Neighbor Discovery (ND), Maximum Transmission Unit (MTU), and MAC layer adaptation.

Vehicles can construct Vehicular Ad Hoc Networks (VANET) by themselves without any infrastructure node such as a Road-Side Unit (RSU). Cooperative Adaptive Cruise Control and Autonomous Driving (i.e., Self-Driving) services can take advantage of this vehicular networking for safe driving through the wireless communications among vehicles.

When using IP-based vehicular networks in self-driving environments, the information exchange among self-driving vehicles are critical to the safety of vehicles since the information received from other vehicles may be used as inputs for vehicle maneuvers. Thus, identifying potential loopholes in the IP-based vehicular networks becomes crucial.

This document describes possible attacks on security and vulnerabilities of privacy in IP Wireless Access in Vehicular Environments (IPWAVE). It also proposes countermeasures for those attacks and vulnerabilities.

2. Terminology

This document uses the definitions defined in the IPWAVE problem statement document [I-D.ietf-ipwave-vehicular-networking].

3. Security Attacks

This section explains possible attacks of security and vulnerabilities of privacy in IP-based vehicular networks.

Security and privacy are very important in V2I, V2V, and V2X communications in vehicular networks. Only identified and authorized vehicles should be allowed to be involved in vehicular networking. Furthermore, in-vehicle devices in a vehicle and mobile devices of a driver and passengers are required to communicate with other devices in VANET or the Internet in a secure and reliable way.

In reality, there are many possible security attacks in vehicular networks. The exemplary security attacks are false information attack, impersonation attack, denial-of-service attack, message suspension attack, tampering attack, and tracking. By these attacks, the vehicles can be put into dangerous situations by false information and information loss.

For those attacks, security countermeasures are required to protect vehicles. With these countermeasures, vehicles can exchange their driving data with neighboring vehicles and infrastructure nodes (e.g., edge computing device and cloud server) for safe driving as well as efficient navigation in road networks.

3.1. False Information Attack

Malicious vehicles may intentionally disseminate false driving information (e.g., location, speed, and direction) to deceive other vehicles, which may put those vehicles in danger. Especially, a representative example is Sybil attack. This Sybil attack makes multiple false identities of non-existing vehicles (i.e., virtual bogus vehicles) in order to confuse other real vehicles in safe driving, and possibly make these real vehicles to make wrong maneuver decisions, leading to fatalities.

A malicious vehicle can also create multiple virtual bogus vehicles, and generate global IPv6 addresses and register them with a Mobility Anchor (MA) via an RSU. This IP address autoconfiguration and registration procedure from many virtual vehicles can occupy the computation power and storage resources of a RSU and an MA and even paralyze the two entities. Thus, the RSU and MA need to determine whether a vehicle is genuine or bogus in the IP address autoconfiguration and mobility management.

3.2. Impersonation Attack

Malicious vehicles can pretend to be other vehicles with forged IP addresses or MAC address as IP address spoofing and MAC address spoofing, respectively. This attack is called impersonation attack to masquerade a vehicle and user.

To detect such an impersonation attack, an authentication scheme needs to check whether the MAC address and IPv6 address of a vehicle is associated with the vehicle's permanent identifier (e.g., a driver's certificate identifier) or not.

3.3. Denial-of-Service Attack

Malicious vehicles (or compromised vehicles) can generate bogus services requests to either a vehicle or a server in the vehicular cloud so that either the vehicle or the server is extremely busy with the requests, and cannot process valid request in a prompt way. This attack is called Denial-of-Service (DoS) attack.

To detect and mitigate this DoS attack, the vehicles need to collaborate with each other to monitor a suspicious activity related to the DoS attack, that is, the generation of messages more than the expected threshold in a certain service.

3.4. Message Suspension Attack

Malicious vehicles can drop packets originated by other vehicles in multihop V2V or V2I communications, which is called a Message Suspension Attack. This packet dropping can hinder the data exchange for safe driving in cooperative driving environments. Also, in multihop V2V or V2I communications, this packet dropping can interfere with the reliable data forwarding among the communicating entities (e.g., vehicle, client, and server).

For the reliable data transfer, a vehicle performing the message suspension attack needs to be detected by good vehicles and a good RSU, and it should be excluded in vehicular communications.

3.5. Tampering Attack

An authorized and legitimate vehicle may be compromised by a hacker so that it can run a malicious firmware or software (malware), which is called a tampering attack. This tampering attack may endanger the vehicle's computing system, steal the vehicle's information, and track the vehicle. Also, such a malware can generate bogus data traffic for DoS attack against other vehicles, and track other vehicles, and collect other vehicles' information.

The forgery of firmware or software in a vehicle needs to be protected against hackers. The forgery prevention of firmware such as the bootloader of a vehicle's computing system can be performed by a secure booting scheme. The safe update of the firmware can be performed by a secure firmware update protocol. The abnormal behaviors by the forgery of firmware or software can be monitored by a remote attestation scheme.

3.6. Tracking

The MAC address and IPv6 address of a vehicle's wireless interface can be used as an identifier. An hacker can track a moving vehicle by collecting and tracing the data traffic related to the MAC address or IPv6 address.

To avoid the illegal tracking by a hacker, the MAC address and IPv6 address of a vehicle need to be periodically updated. However, the change of those addresses needs to minimize the impact of ongoing sessions on performance.

4. Security Countermeasures

This section proposes countermeasures against the attacks of security and privacy in IP-based vehicular networks.

4.1. Identification and Authentication

Good vehicles are ones having valid certificates (e.g., X.509 certificate), which can be validated by an authentication method through an authentication server [RFC5280].

Along with an X.509 certificate, a Vehicle Identification Number (VIN) can be used as a vehicle's identifier to efficiently authenticate the vehicle and its driver through a road infrastructure node (e.g., RSU and MA), which is connected to an authentication server in vehicular cloud. X.509 certificates can be used as Transport Layer Security (TLS) certificates for the mutual authentication of a TCP connection between two vehicles or between a vehicle and a corresponding node (e.g., client and server) in the Internet.

Good vehicles can also use a Decentralized Identifier (DID) with the help of a verifiable claim service. In this case, vehicles can their DID as a unique identifier, and then check the identity of any joining vehicle with its verifiable claim.

4.2. Integrity and Confidentiality

For secure V2I or V2V communications, a secure channel between two communicating entities (e.g., vehicle, RSU, client, and server) needs to be used to check the integrity of packets exchanged between them and support their confidentiality. For this secure channel, a pair of session keys between two entities (e.g., vehicle, RSU, MA, client, and server) needs to be set up.

For the establishment of the session keys in V2V or V2I communications, an Internet Key Exchange Protocol version 2 (IKEv2) can be used [RFC7296]. Also, for the session key generation, either an RSU or an MA can play a role of a Software-Defined Networking (SDN) Controller to make a pair of session keys and other session parameters (e.g., a hash algorithm and an encryption algorithm) between two communicating entities in vehicular networks [RFC9061].

4.3. Non-Repudiation

A malicious vehicle can disseminate bogus messages to its neighboring vehicles as a Sybil attack. This Sybil attack announces wrong information of a vehicle's existence and mobility information to normal vehicles. This may cause accidents (e.g., vehicle collision and pedestrian damage). In the case of the occurrence of an accident, it is important to localize and identify the criminal vehicle with a non-repudiation method through the logged data during the navigation of vehicles.

For non-repudiation, the messages generated by a vehicle can be logged by its neighboring vehicles. As an effective non-repudiation, a blockchain technology can be used. Each message can be treated as a transaction and the adjacent vehicles can play a role of peers in consensus methods such as Proof of Work (PoW) and Proof of Stake (PoS) [Bitcoin].

4.4. Remote Attestation

To prevent a tampering attack by the forgery of firmware/software, a secure booting can be performed by Root of Trust (RoT) and a remote attestation can be performed through both the secure booting and RoT [I-D.pastor-i2nsf-nsf-remote-attestation][I-D.ietf-rats-architecture].

The secure booting can make sure that the bootloader of the vehicle's computing system is a legitimate one with the digital signature of the boofloader by using the RoT of Trusted Platform Module (TPM) [ISO-IEC-TPM] or Google Titan Chip [Google-Titan-Chip].

A firmware update service can be made in blockchain technologies [Vehicular-BlockChain]. The validity of a brand-new firmware can be proven by a blockchain of the firmware, having the version history. Thus, This blockchain can manage a brand-new firmware or software and distribute it in a secure way.

The remote attestation can monitor the behaviors of the vehicle's computing system such that the system is working correctly according to the policy and configuration of an administrator or user [I-D.pastor-i2nsf-nsf-remote-attestation][I-D.ietf-rats-architecture]. For this remote attestation, a secure channel should be established between a verifier and a vehicle.

4.5. Privacy

To avoid the tracking of a vehicle with its MAC address, a MAC address pseudonym can be used, which updates the MAC address periodically. This update triggers the update of the vehicle's IPv6 address because the IPv6 address of a network interface is generated with the interface's MAC address. The MAC address and IPv6 address can be updated by the guideline in [RFC4086] and a method in [RFC4941], respectively.

The update of the MAC address and the IPv6 address affects the on-going traffic flow because the source node or destination node of the packets of the flow are identified with the node's MAC address and IPv6 address. This update on a vehicle requires the update of the neighbor caches of the vehicle's neighboring vehicles for multihop V2V communications, as well as the neighbor caches of the vehicle's neighboring vehicles and the neighbor tables of an RSU, and an MA in multihop V2I communications.

Without strong confidentiality, the update of the MAC address and IPv6 address can be observed by an adversary, so there is no privacy benefit in tracking prevention. The update needs to be notified to only the trustworthy vehicles, RSU, and MA.

Also, for the continuity of an end-to-end (E2E) transport-layer (e.g., TCP, UDP, and SCTP) session, the new IP address for the transport-layer session can be notified to an appropriate end point through a mobility management scheme such as Mobile IP Protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275] and Proxy MIPv6 (PMIPv6) [RFC5213]). This mobility management overhead and impact of pseudonyms should be minimized on the performance of vehicular networking.

5. Security Considerations

This document discussed security considerations for IPWAVE security and privacy in Section 3 and Section 4.

6. References

6.1. Normative References

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", DOI 10.17487/RFC4086, RFC 4086, BCP 106, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <https://www.rfc-editor.org/info/rfc4941>.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <https://www.rfc-editor.org/info/rfc5213>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", DOI 10.17487/RFC6275, RFC 6275, July 2011, <https://www.rfc-editor.org/info/rfc6275>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8691] Benamar, N., Härri, J., Lee, J., and T. Ernst, "Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11", RFC 8691, DOI 10.17487/RFC8691, December 2019, <https://www.rfc-editor.org/info/rfc8691>.

[RFC9061] Marin-Lopez, R., Lopez-Millan, G., and F. Pereniguez-Garcia, "A YANG Data Model for IPsec Flow Protection Based on Software-Defined Networking (SDN)", RFC 9061, DOI 10.17487/RFC9061, July 2021, <https://www.rfc-editor.org/info/rfc9061>.

[I-D.ietf-ipwave-vehicular-networking]
Jeong, J. P., "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", Work in Progress, Internet-Draft, draft-ietf-ipwave-vehicular-networking-29, 19 May 2022, <https://www.ietf.org/archive/id/draft-ietf-ipwave-vehicular-networking-29.txt>.

6.2. Informative References

[I-D.pastor-i2nsf-nsf-remote-attestation] Pastor, A., Lopez, D. R., and A. L. Shaw, "Remote Attestation Procedures for Network Security Functions (NSFs) through the I2NSF Security Controller", Work in Progress, Internet-Draft, draft-pastor-i2nsf-nsf-remote-attestation-07, 11 February 2019, <https://www.ietf.org/archive/id/draft-pastor-i2nsf-nsf-remote-attestation-07.txt>.

[I-D.ietf-rats-architecture] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", Work in Progress, Internet-Draft, draft-ietf-rats-architecture-19, 24 July 2022, <https://datatracker.ietf.org/api/v1/doc/document/draft-ietf-rats-architecture/>.

[ISO-IEC-TPM] ISO/IEC JTC 1, "Information technology - Trusted Platform Module - Part 1: Overview", ISO/IEC 11889-1:2015, August 2015.

[Google-Titan-Chip] Google, "Titan in depth: Security in plaintext", URL: https://cloud.google.com/blog/products/gcp/titan-in-depth-security-in-plaintext, October 2018.

[ISO-ITS-IPv6] ISO/TC 204, "Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking", ISO 21210:2012, June 2012.

[DSRC] ASTM International, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ASTM E2213-03(2010), October 2010.

[WAVE-1609.0] IEEE 1609 Working Group, "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture", IEEE Std 1609.0-2013, March 2014.

[IEEE-802.11-OCB] "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2016, December 2016.

[Bitcoin] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", URL: https://bitcoin.org/bitcoin.pdf, May 2009.

[Vehicular-BlockChain] Dorri, A., Steger, M., Kanhere, S., and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy", IEEE Communications Magazine, Vol. 55, No. 12, December 2017.

Appendix A. Acknowledgments

This work was supported in part by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (2020-0-00395-003, Standard Development of Blockchain based Network Management Automation Technology).

This work was supported in part by the MSIT under the ITRC (Information Technology Research Center) support program (IITP-2022-2017-0-01633) supervised by the IITP.

Appendix B. Contributors

This document is made by the group effort of IPWAVE working group. Many people actively contributed to this document, such as Carlos J. Bernardos and Russ Housley. The authors sincerely appreciate their contributions.

The following are co-authors of this document:

Bien Aime Mugabarigira - Department of Electrical and Computer Engineering, Sungkyunkwan University, 2066 Seobu-ro Jangan-gu, Suwon, Gyeonggi-do 16419, Republic of Korea. EMail: bienaime@skku.edu

Zhong Xiang - Department of Electrical and Computer Engineering, Sungkyunkwan University, 2066 Seobu-ro Jangan-gu, Suwon, Gyeonggi-do 16419, Republic of Korea. EMail: xz618@skku.edu

Appendix C. Changes from draft-jeong-ipwave-security-privacy-05

The following changes are made from draft-jeong-ipwave-security-privacy-05:

*This version updates the author list.

Authors' Addresses

Jaehoon Paul Jeong (editor)
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4957
Email: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Yiwen Chris Shen
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4106
Email: chrisshen@skku.edu
URI: https://chrisshen.github.io

Hyeonah Jung
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4106
Email: hyeonah214@skku.edu

Jung-Soo Park
Electronics and Telecommunications Research Institute
218 Gajeong-Ro, Yuseong-Gu

Daejeon
34129
Republic of Korea

Phone: +82 42 860 6514
Email: pjs@etri.re.kr

Tae Tom Oh
Golisano College of Computing and Information Sciences
Rochester Institute of Technology
One Lomb Memorial Drive
Rochester, NY 14623-5603
United States of America

Phone: +1 585 475 7642
Email: Tom.Oh@rit.edu