ITS Working Group
Internet-Draft
Intended Status: Standards Track
Expires: January 7, 2017

Minpeng Qi
China Mobile

July 7, 2016

Authentication Problem Statement for Vehicle-to-Vehicle Communication
draft-qi-its-v2vauth-00

Abstract

This document specifies the problem statement for authentication issue analysis in the vehicle-to-vehicle communication. It gives privacy protection and certification considerations for authentication designing.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Table of Contents

1 Introduction

During the V2V communication, attacker could personate as a legal vehicle to communicate with others if there is no authentication. Attackers could also sends any fake message out, or collect sensitive information without any worries to be caught. It will pollute the environment for V2V communication. As a result, authentication is needed for V2V.
This document considers some authentication issues raised in V2V environment, including privacy and certification usage.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2 Privacy consideration in authentication

Privacy is very important for V2V communication. During V2V communication, the peer could bind vehicle's identity and location together. This will cause tracking problem. So vehicle's effective identity MUST NOT be revealed to the peer. However, as mentioned above, vehicle could not be as completely anonymous when communicate with the peer, as this will lead to illegal behavior happening. So privacy protection should be designed carefully.

A possible compromised mechanism is using a temporary identity instead of vehicle's real identity, or could be recognized as permanent identity, in the communication process. The temporary ID MUST be able to be bound with permanent ID in some way. The binding relationship SHOULD be revealed to specified 3rd party and could be traced back under some situation. If not, it means temporary ID could not be bound with permanent ID, or the binding relationship is only kept with the vehicle. This permanent ID could be seen as another kind of anonymous ID, because it will cause permanent ID could not be traced back when attacking is happened with such temporary ID. And that's should be prevented. So temporary ID must be bound with its permanent ID and be revealed. As a result, this temporary ID could be considered as a pseudonym. For example, when using certificate in authentication, common name in certificate could be seen as such pseudonym, the information registered in CA for certificate issuing could be seen as such permanent ID. CA could be seen as the 3rd part to keep the binding relationship. And this should also be applied for other solution when certificate is not used in authentication.

In another aspect, a temporary ID should not be available with a long time. Privacy in a nutshell encompasses the inability for any entity

to track a vehicle UE beyond a short (e.g. 5 minutes) time interval.

3 Security Considerations

For mutual authentication of V2V communication, the easiest implementation is using certificate. All vehicles own certificates and send its proper certificates or certificate chain to the peer in order to prove its identity.

Considering different certificate issued to different vehicles by different CA, vehicle should maintain a lot of certificates of root CA, which is used for verify certificate sent by the peer. However, in some regions/area/countries where vehicles are manufactured, vehicle may be required to hold certificate issued by special CA. This leads problem that those vehicle may be not able to be verified when communicates with other vehicles, as the other vehicles may not have certificate for such special root CA.

Another problem is raised for delay time. The time window is small for V2V communication due to the high movement of vehicles. It has strict requirement as such communication could be seen as real-time communication. However, when vehicle gets certificate chains from the peer, it should verify each certificate in the chain to get the result. It will cause time consuming.

Another issue for certificate is validity period. It the period is too long, the leaking risk will be raised. Then compromised certificate should be revoked. If we need to consider such issue, additional mechanism should be introduced in vehicle, such as OCSP, or CRL. Vehicle should be able to verify the validity of received certificate from peers through OCSP protocol. Connecting CA is needed in this case. Applying OCSP protocol will cause additional delay in authentication. So it is not very fit for V2V communication scenarios. Or it should be able to maintain a CRL database. When using CRL, vehicle needs to download CRL file before using it, or when the old file is out of date. This is similar like using OCSP. What is more, maintenance of CRL database will require additional storage. It is not advisable as vehicle's performance is usually limited. Therefore, when certificate is used in authentication, the validity of certificates needs to be set in a reasonable range. With fast expiration of certificates, the risk of leakage could be reduced. And it could avoid checking the validity of certificate. In another aspect, the privacy protection also requires short certificate validity time, as common name needs to be changed in short time.

However, it the validity time is too short, it also has some problems. It requires CA should issues certificate issuing very frequently. So it requires vehicle should communicate with CA in a frequent way, nearly like always online. But this requirement is hardly fulfilled. When vehicle is driven outside in the wild, it is difficult to keep the connection between vehicle and CA. There is another option, that

CA could issue a bulk certificates to vehicle. Such certificates have

different expiration times to implement time interval. In this way, vehicle needs to maintain many certificates. If CA will issue all certificates expired in a year once, and the time interval is 5 minutes as mentioned above (in privacy section), it means more than 100,000 certificates should be stored in vehicle. That's huge burden for vehicle. What is more, such certificates should be used one by one, with validate time sequence strictly. This will bring more cost for vehicle implementation. But it still has same problem that certificate could be leaked, especially for the certificates whose expiration date is longer.

In a word, if we want to use certificate in authentication, a new mechanism for certificate fitting for V2V communication is needed, which should covers certificate's generation, issue, verification, validation and revocation. Or some attached mechanism for certificate should be designed.

4 Authentication by using other credential

TBD.
(This section should consider problems raised by any other mechanism without using certificate.)

5 Security Consideration

This documents are specifies security issues.

6 Acknowledgements

7 References

Authors' Addresses

Minpeng Qi
China Mobile
32 Xuanwumenxi Ave,Xicheng District
Beijing 100053
China

Email: qiminpeng@chinamobile.com