Indian Journal of Science and Technology, *Vol 8(15), IPL034, July 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A TPM-based Architecture to Secure VANET

Jadhav Shital Suresh* **and Lee Jongkun**

Department of Computer Engineering, Changwon National University, Gyeongsangnam-do, South Korea;
jadhavlike@gmail.com, jklee@changwon.ac.kr

Abstract

Vehicular Ad hoc Network (VANET) is a special network of vehicles which can communicate with one another on the roads. Now days, VANET get increased attention by vehicle manufactures and researchers. However their deployment requires that security and privacy issues to be resolved, since they rely on wireless communication. In this paper, we are going to represent that security architecture built around TPMs can provide satisfactory solution. Moreover, this architecture does not require deployment of base stations along the roads. We will also show that how hardware device like USB memory stick will improve the anonymity in order to prevent unauthorized vehicle tracking.

Keywords: Anonymity, Security, Trusted Platform Module (TPM), Vehicular Ad hoc Network (VANET)

1. Introduction

Last few years, Vehicular Ad hoc Network (VANET) is receiving a lot interest due to variety of services that they can offer. The most important goal of VANET is to enable public safety applications that can potentially save lives and improve traffic conditions. VANETs are highly dynamic ad hoc network with very limited access to an infrastructure. In addition, if base stations are practically deployed in real time scenario along the road then access is of short duration because of vehicle speed which is not constant. The absence of a permanently accessible infrastructure means that decentralized architecture is necessary[1–3]. If we assume that deployment of RSU will take time then there is need to find out the solution without RSU. Also safety is most important application in VANET; we need security architecture which must prevent a malicious attack which is aims to collisions between vehicles.

Hardware plays a very important role to provide a security in vehicular environment. In this paper, we contend that the system requirements like confidentiality, integrity and availability can be fulfilled by a security architecture built around Trusted Platform Module (TPM). TPM used to verify that correct functioning of software of a vehicle and the distribution of keys for TPM operation can be accommodate by current vehicle registration and maintenance by current vehicle registration and maintenance practices. We use a memory stick carried by the driver from a PC with an internet connection (Home, Office) to the vehicle, as shown in Figure 1 taken from[4]. The solution proposed in this paper is based on keys preloaded in the vehicle during the construction phase and a protocol using the memory stick to renew the certified keys.

In section 2, we will present related work. In section 3, we will analyze the threat model and section 4 we present our solution and basic architecture of TPM. Section 5 describes the various communication protocols used between the different components of the proposed architecture. Section 6 concludes the paper.

2. Related Work

The open nature of a VANET makes communication security a great challenge[5,6]. In VANET, it is very easy to modify or inject faulty data by malevolent node because data is transmitted over a shared communication media.

Vehicular Public Key Infrastructure (VPKI)[7,8] is an approach to VANET security which is based on a public key infrastructure and base stations along the road. Both solutions are able to provide the support for key distribution and revocation. VPKI solutions provides the direction

*Author for correspondence

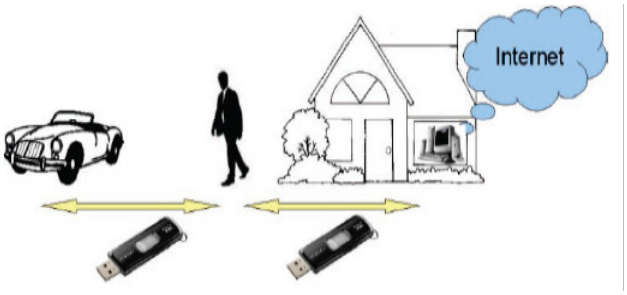

Figure 1. The USB memory sticks as TPM.

to tackle the problem of privacy such as car tracking by using an anonymous key set and key changing algorithm. However, the PKI deployment is large-scale and costly procedure under real-world VANET conditions.

Some other papers address the problem of privacy[9–11]in VANET with the help of infrastructures (base stations and certification authorities) and pseudonym use [11] deals with the challenges encountered when applying anonymity to a VANET communication system and propose a framework for pseudonymity support.

Most related work is based on a set of keys or pseudonyms which induces the overhead on the certificate authority and there is need to find out solution which will overcome these issues.

3. Thread Model

As mentioned, the security architecture must meet the system requirements like confidentiality (the content of the message should be secure and should not be accessible to attackers), integrity (the content of the message should not alter from sender to receiver) and availability (when any vehicle wants to gain access the other vehicle in the network or access the infrastructure, the network is not available to user due to some kind of attack). Generally security architecture has to deal with the following attacks.

3.1 The Sybil Attack

The Sybil attack was first described by Douceur in[12]. In this type of attack, attacker send multiple messages which contains different fabricated source identity to other vehicles. It confuses other vehicle by sending some wrong messages like traffic jam messages. Applications of the Sybil attack to Vehicular Ad-Hoc Networks are discussed in[16,17] and show the importance of Sybil node detection in VANETs.

Figure 2 explains Sybil attack in which the attacker creates multiple vehicles on the road with the same identity. The objective of a Sybil attack is to leave the road by other vehicles, for the benefits of attacker. Sybil attacks are always possible (i.e. may remain undetected) except under the extreme and unrealistic assumption of resource parity and coordination among entities.

3.2 Node Impersonation

The drivers are legally responsible for their actions behind the wheel for e.g. in case of an accident or a driving offense. This is possible because of database of driving license plates. In VANET, each vehicle has a unique identifier which is used to verify the messages. This unique identifier must be protected so that an attacker cannot impersonate with some other car's identity. The Figure 3 shows that vehicle A involves in the accident at location z. When police identify the driver by using driver's identity, attacker changes his identity and simply refuses it.

3.3 Car Tracking

In this type of attack, the attacker monitors the whole network and listen the communication between V2V and V2I. By doing this, there is possibility of getting some related information. In this case, the attacker can pass this related information to the concerned person.

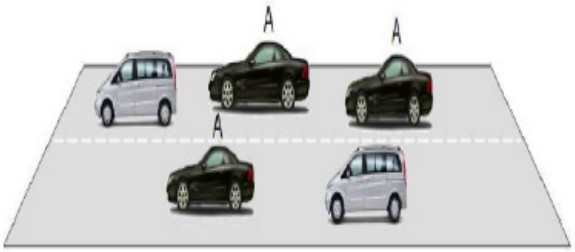

Figure 2. The Sybil Attack.

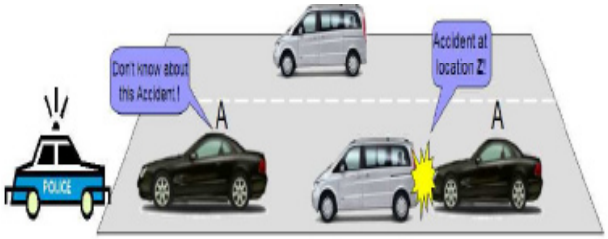

Figure 3. Node Impersonation.

For e.g. police are plan to perform some operation against criminal and they communicate each other and guide about the exits location of the operation. Attacker listen all communication and informed the criminal about the police operation. Every vehicle has its own unique ID and attacker disclose the identity of other vehicles in the network. The attacker can track the existing location of vehicle with the help of unique ID. Figure 4 shows this type of scenario.

3.4 Basic Security Properties

Below are some basic properties that a security solution must provide to overcome above threats.

Property 1 : A vehicle must have a unique identifier.
Property 2 : Each message must be authenticated with regards to a vehicle identifier and integrity of this message must be ensured.
Property 3 : The trustfulness of message contents must be verifiable.

To implement these security properties, a vehicle have to establish trust in another vehicle even though that vehicle is under complete control of an untrusted driver. Therefore we require the solution which uses the secure hardware.

4. The Trusted Platform Module

A general purpose hardware chip designed for secure computing is the Trusted Platform Module (TPM)[13] which can be integrated into any device. TPMs are now shipped with PCs; 200 million TP-enabled PCs have been shipped by the end of 2007.

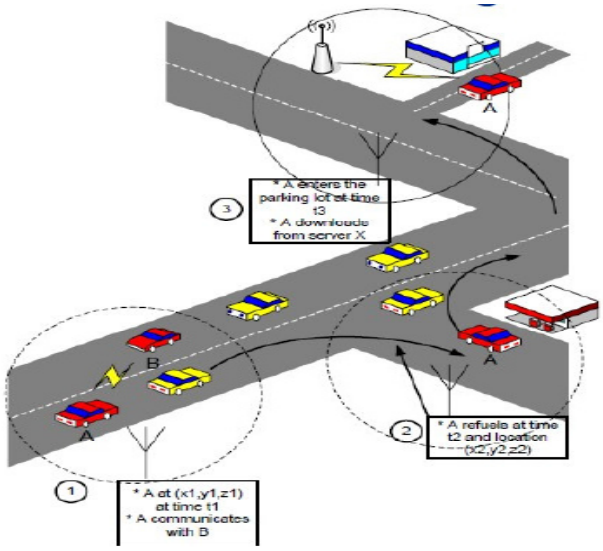

Figure 4. Car Tracking Scenario.

4.1 Introduction

A TPM is a piece of hardware, requiring a software infrastructure, which is able to protect and store data in shielded locations. A TPM has also cryptographic capabilities such as SHA1 engine, an RSA engine and a random number generator. Figure 5, taken from[13], illustrate the main components of a TPM. TPM is able to store the system hardware and software configuration in a specific shielded location called a Platform Configuration Register (PCR). If any change attacker tries to make into application then this will lead change in the PCR values, thus it will allow to detect that the application get hacked.

There are several keys used by a TPM for authentication purpose and attestation. They are as follows:

- **The Endorsement Key (EK):** This is unique master key which is securely stored inside the TPM. This is a pair of RSA keys with a minimum size of 2048 bits. The public part of the EK is available in the Endorsement certificate. EK is generated by the TPM constructor.
- **The Attestation Key (AIK):** This is RSA key pairs generated by the TPM on multiple bases. It is used for attestation of current platform and its configuration i.e. TPM. Privacy Certification Authority (PCA) and Direct Anonymous Attestation (DAA) are used for certification of attestation of AIK. One advantage of AIK is that it does not disclose the identity of the TPM.

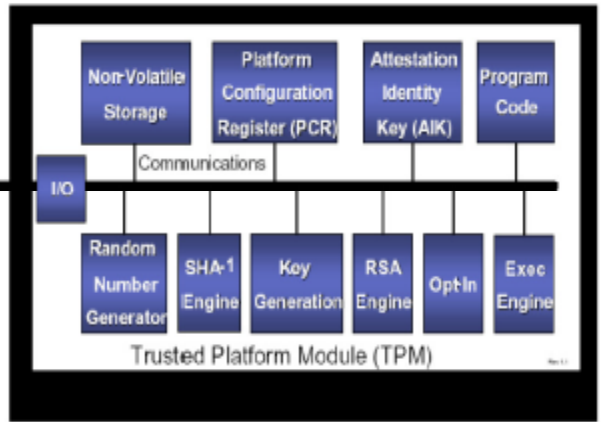

Figure 5. Architecture of a TPM.

4.2 Embedded Architecture

In VANET, main communication is divided into two parts. First, embedded sensors communicate with the applications and second are applications communicate with the TPM for data siging purposes. This type of communication is also konwon as Inside communication which is used to sign data and keep data safe in secure location. Figure 6 shows the different components of the embedded architecture and data flow[14]. Sensors embedded within a vehicle give results of their measures to the application. Then application asks TPM to sign the data. TPM checks the PCR values associated with this application and sign data provided by the application. Then the application can store this data in a dedicated repository. The proposed solution is based on several cryptographic key pairs pre-loaded in the vehicle during construction phase. These key pairs later are used by a specific protocol to build the cryptographic pseudonyms. Also a memory stick can be used to renew the key pairs in an opportunistic manner.

In the section V, we will see different protocols which are used for communication and data sigining purposes.

5. Protocols

5.1 Attestation Protocol

Attestation is the system ability to confirm the integrity of certain types of information or evidence. In TPM context, evidence is nothing but the PCR values. The TPM provides two modes for anonymous attestation: PCA based and DAA based.

5.1.1 PCA based Attestation Protocol

Privacy Certification Authority (PCA) is a trusted third party which issues the certificate for AIK and verifies the AIK. When the PCA receives the public part of EK sent by TPM, the PCA verifies the information. If the information is valid then it will create a certified secondary key pair AIK and send this credential back to requestor. The purpose of this is to provide the user with anonymity. When the user has this certified AIK, user can able to communicate with other trusted platforms. Figure 7 shows the process for this protocol.

5.1.2 DAA based Attestation Protocol

The TCG have developed a new method to obtain the certified AIK. This process is called DAA (Direct Anonymous Attestation). DAA is digital group signature scheme and it was originated by Brickell, Camenisch and Chen[15]. The Figure 8 describes the process mechanism of DAA.

This method does not require the user to disclose his/her public part of EK. DAA is a digital group signature scheme. It provides the facility to third party for the validation of TPM and to check platform is genuine or not. Before the TPM can send a certification request from an AIK to the remote entity, the TPM has to generate a set of DAA credentials. This can be achieved by interacting with an issuer. This is the joining process. The DAA credentials are created by the TPM sending a TPM-unique secret is similar but not analogous to the EK, The computation of secret key and identity of issuer is done by the discrete algorithm (Zero-knowledge proof of knowledge). When the TPM has obtained a set of DAA credentials, it can

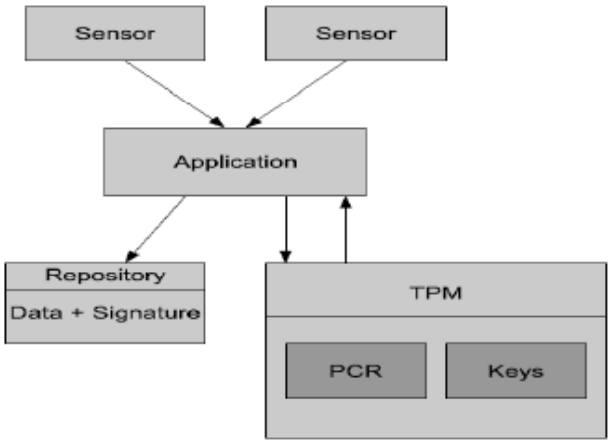

Figure 6. Embedded Architecture.

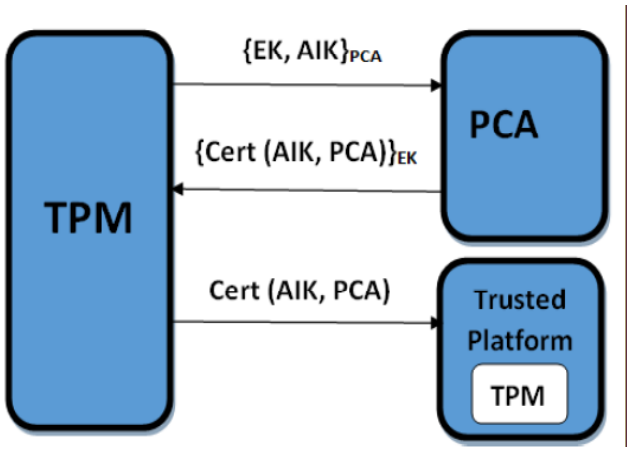

Figure 7. PCA-based Attestation Protocol.

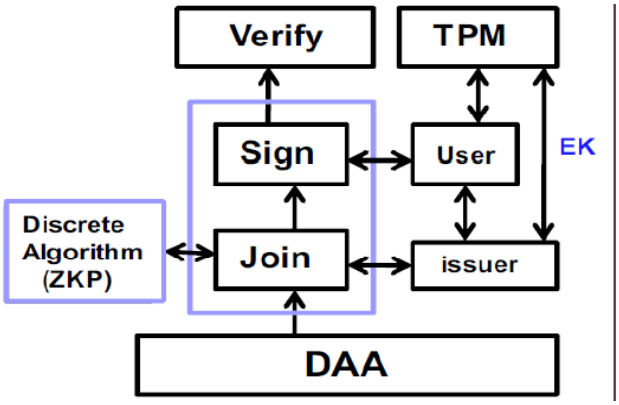

Figure 8. Process mechanism of DAA based Attestation protocol.

send these to the signer. DAA signer is combination of TPM and user, they work together. It is used to allow the user to authenticate the message on the base of signature. Now, user signs the message and generates the signature. When the verifier receives the DAA credentials and signature from the trusted third party, it will verify them and send a certified AIK back to the user. By using these certified AIK, user will be able to communicate with other trusted parties. In this case, the verifier may or may not be a trusted third party. Now the verifier can determine that the DAA credentials are valid or not. This DAA credentials does not contain any unique information related to the TPM platform. In summary a separate entity that will assist in the anonymous attestation process. DAA issuer mostly will be the TPM manufacturer and it protects the user anonymity towards the verifier or TTP. Without such DAA credentials, it will be possibly more difficult to convince other vehicle that they have a genuine trusted platform.

5.2 The Challenge-response Protocol

Vehicles can challenge to each other to detect unintentional errors. The detail of this is given in Figure 9. The challenger can ask about data it can verify, for e.g. the current position. Then the challenged vehicle collects the appropriate data, gives this data to its TPM. Then TPM checks the PCR values which are associated with the application and signs data. After this application sends the signed data and associated credential to the challenger. At the end, the challenger verifies the signature and compares the given position to its own current position to detect any problem within positioning unit of the challenged vehicle.

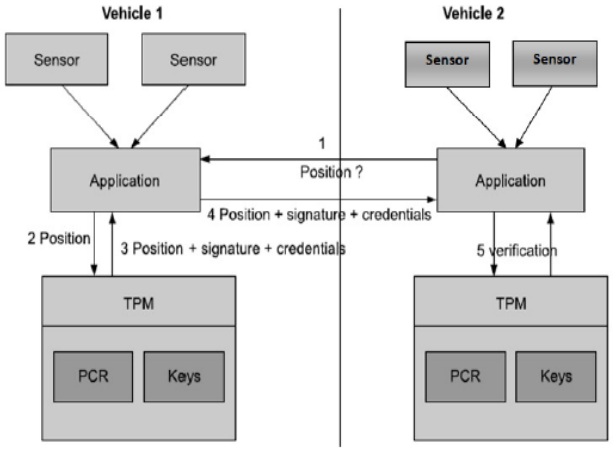

Figure 9. Challenge-Response Protocol.

5.3 Anonymity Revocation

Adding anonymity in the inter-vehicle communications must not prevent the authorities to catch the attacker in given situations. This is important for the deployment of a realistic solution. We believe in particular that a solution without a trap will not be accepted in the automotive world when the driver engages its liability. We can underline that current registration system offer exactly this type of feature. The registration provides anonymity for everyone and only one entity can associate the license plate number with the identity of the driver.

We have introduces an additional parameter i.e. secret key in the certificate of an AIK. Because of this setting an authority who knows this secret key can be able to retrieve the information related to the vehicle like registration number.

5.4 Key Revocation

There are two types of keys which can be revoked in our model like AIK and EK.

When PCA will get informed of a compromised AIK then it simply updates the revocation list accordingly. We use an opportunistic revocation mechanisms the vehicle request and obtain RL via memory stick. Because of this the primary function of TPM is no longer fulfilled. So PCA will place the EK in the revocation list and keep the information locally in order not to certify further AIK for this TPM.

If the driver never uses the memory stick, then the revocation list is never provided to the vehicle. Thus, the vehicle may unnecessary verify some messages crafted with revoked keys.

6. Conclusion

In this paper, we have presented the benefits provided by the TPM architecture in VANET. We show a way to use a TPM component embedded in vehicles to improve security and anonymity of VANET communication. In the PCA based solution, the connection with the PCA is enforced by a memory stick. This device requires the involvement of the driver and can be a problem for the deployment. If we make no assumption about the security of the opportunistic communication between the vehicle and the network then we can use of other types of communication such as a 3G phone in the vehicle that connects to the PCA via a GSM communication. In the case of DAA based protocol it does not need a certification authority. This scheme develops the chain of trust and also to solve the problem of privacy of users while communicating with other vehicles. In this way, the lower cost of this module and their functionality in VANET will make the implementation of this technology easier.

7. References

1. Conti M, Giordano S. Multihop ad hoc networking: the theory. IEEE Communications Magazine. 2007; 45(4): 78–86.
2. Blum J, Eskandarian A. The threat of intelligent collosions. IT Professional. 2004 Jan-Feb; 6(1):24–9.
3. EI Zarki M, Mehrotra S, Tsudik G, Venkatasubramanian N. Security issues in a future vehiclar network. European Wireless. 2002; p. 270–74.
4. Guette G, Heen O. A TPM-based architecture for improved security and anonymity in vehicular ad hoc networks. IEEE Vehicular Networking Conference (VNC); France: IRIS; 2009.
5. Zarki ME, Mehrotra S, Tsudik G, Venkatasubramanian N. Security issues in a future vehicular network. European Wireless; 2002.
6. Parno B, Perrig A. Challenges in securing vehicular networks. 4th Workshop on Hot Topics in Networks; 2005 Nov; Association for Computing Machinery Inc.
7. Raya M, Hubaux J. The security of vehicular ad hoc networks. Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks; 2005. p. 11–21.
8. Raya M, Papadimitratos P, Hubaux J. Securing vehicular communications. IEEE Wireless Communications Magazine. 2006; 13(5):8–15.
9. Dotzer F. Privacy issues in vehicular ad hoc network. Workshop on Privacy Enhancing Technologies; 2005. p. 197–209.
10. Gerlach M, Festag A, Leinmuller, T, Goldacker G, Harsch C. Security architecture for vehicular communication. Workshop on Intelligent Transportation; 2007.
11. Fonseca E, Festag A, Baldessari R, Aguiar R. Support of anonymity in vanets-putting pseudonymity into practice. IEEE Wireless communications and Networking Conference. 2007 Mar 11-15; Kowloon; p. 3400–05.
12. Douceur J. The Sybil Attack. First International Workshop on Peer-to-Peer Systems; 2002. p. 251–60.
13. Trusted Computing Group: TPM main Specification. Main Specification Version 1.2 rev. 85. Trusted Computing Group. 2005 Feb.
14. Guette G, Bryce C. Using tpms to secure Vehicular Ad hoc Networks (VANETs). Workshop on Information Theory and Practices; 2008. p. 106–16.
15. Brickell E, Camenisch J, Chen L. Direct anonymous attestation. Proceedings of 11th ACM Conference on Computer and Communications Security; New York, NY, USA: ACM Press; 2004. p. 132–45
16. Blum J, Eskandarian A. The threat of intelligent collisions. IT Professional. 2004; 6(1):24–9.
17. Raya M, Hubaux J. Securing Vehicular Ad Hoc Networks. Journal of Computer Security - Special Issue on Security of Ad Hoc and Sensor Networks. 2007; 15(1):39–68.