

Distributed Certificate Architecture for VANETs

Baber Aslam and Cliff C. Zou

School of Electrical Engineering and Computer Science
University of Central Florida
Orlando, FL, USA

{ababer, czou}@eecs.ucf.edu

ABSTRACT

Privacy, authentication, confidentiality and non repudiation are the most desired security attributes for all vehicular ad hoc network (VANET) applications. A lot of solutions have been presented to address these issues; many of them are quite comprehensive and address most of the security requirements. However, they are mostly dependent on centralized certificate architecture and some sort of hardware security. These solutions are expensive to carry out and lack the incentive for users to deploy, which make them especially difficult to be implemented during the initial deployment stages of VANET.

We present distributed security architecture for VANET that does not rest on expensive security hardware or elaborate security architecture. The architecture can be incrementally deployed and can fill the void during the initial deployment phase. Our solution is based on time/space restricted certificates, which are issued upon user's request and can be used for various VANET applications. Due to restricted nature of these certificates, the revocation process is simple and efficient, which solves another drawback of existing solutions.

Categories and Subject Descriptors

C.2.0 [General]: Security and Protection; C.2.1 [Network Architecture and Design]: Wireless Communication

General Terms

Security, Design.

Keywords

Security, privacy, VANET, vehicular networks.

1. INTRODUCTION

All VANET applications either collect or disseminate information from/to vehicles. The authenticity of the information is very important since malicious information may result in loss of life and property. This authenticity of information can be achieved, if some means of liability are introduced. Besides non repudiation; confidentiality, privacy and authentication are the desired security attributes. The best possible solution is to use digital certificates tied to a user/provider by a trusted third party. These certificates can then be used to sign the information. Most of the existing solutions use some kind of certificates with a central certificate-issuing/trusted authority [1-5]. To protect the privacy the architecture can be extended to use many temporary certificates (or called pseudonyms) instead of one permanent certificate. These pseudonyms can be stored in bulk (in a temper proof device

- TPD [2]), issued by an online authority [3,4] or generated by user himself [5].

The centralized certification authority (CA) based solutions present a number of challenges which may be difficult to address during the initial deployment stages of VANET. The CAs must be organized in a hierarchical manner for effective management and a trust relationship must exist among regional CAs. This means certificate verification may take longer especially if the trust relationship goes through a long chain. Further, it also makes revocation difficult since revocation list (RL) must be distributed to all regions as vehicles are not restricted to remain within their regions. The RL may grow over time, making its distribution more difficult. Papadimitratos et al, suggested restricting the scope of RL within a region, requiring visiting nodes from other regions to obtain temporary certificates [6].

Too much trust is placed on TPD, which stores permanent certificate and pseudonyms; vehicle cannot be physically guarded as other electronic security devices (smart cards etc). This requirement will make the device quite expensive [7]. Further, the pseudonyms when exhausted must be reloaded thus requiring a periodic maintenance.

To address these challenges, we propose a distributed certificate architecture. Certificates with a limited temporal/spatial scope are issued by a service provider. These certificates are usable within a particular geographic area or within a certain time or both. These certificates are not tied to the vehicle's registration etc and can be changed periodically during one service period. Meanwhile law enforcement agencies can trace back the user via the temporary certificate and the service provider.

2. ARCHITECTURE

The basic idea is that if a user wants to participate in a VANET (the user's vehicle is not required to have a manufacturer's issued certificate), he purchases a payment-processing-device (similar to automatic toll payment devices - sold for tens of dollars). Each device will have an identification and an associated certificate. During initialization the device will be linked/registered with the user's account; user's information will be maintained with the provider and will not be stored in the device. The basic procedure is illustrated in Fig 1. When a user enters a service area and wants to use the service, he makes the payment for the service using onboard payment device. The payment-authorization/service-request message will be encrypted using provider's public key, thus hiding the device ID/certificate and services requested from eavesdroppers. The user is issued a pseudonym and other IDs necessary for the service by the provider. The concerned server is also informed of the service purchased and temporary credentials. The temporary credentials can also be used to provide desired

security attributes for VANET applications including vehicle to vehicle -V2V communications. As a baseline service, the user can obtain just the temporary credentials, in this case the temporary credentials will not be sent to servers.

Certificate, IP address, MAC address etc can all be issued on temporary basis and refreshed several times during a service period. They are encrypted to ensure security and privacy. Initially, they can be encrypted using a random session key sent along the request. Later, they can be encrypted using current public key.

The certificate of CA is hard coded in the device, enables other users to check validity of a certificate. Methods can be employed to safeguard against replay, spoofing, man-in-the-middle etc. attacks.

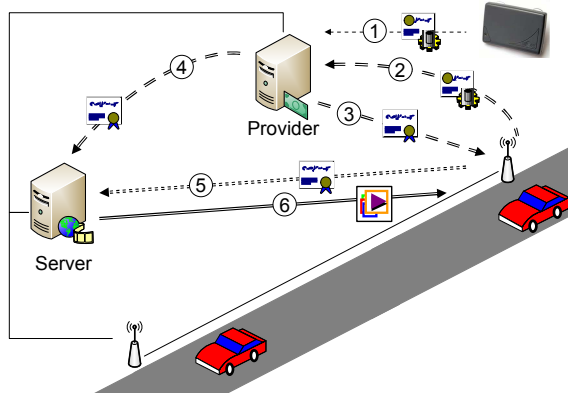


Figure 1: Architecture (1) User registers device with provider (2) User sends payment/service request (3) Provider issues temporary credentials (4) Provider informs server of service purchased and temporary credentials (5) User requests service using temporary credentials (6) Server delivers content.

3. ANALYSIS

The architecture ensures desired security attributes. Authentication and confidentiality can be achieved by signing/encrypting the messages using associated public keys. Attacker cannot link the pseudonyms with a user; even different pseudonyms cannot be linked with each other, thus ensuring privacy. Liability can be enforced with the help of payment processing provider, since it has the account information for each issued pseudonym.

The architecture, as opposed to existing solutions, does not require users to maintain permanent or valid temporary certificates when they are not using the service; user purchases a certificate only when he wants to use the service. The architecture also simplifies the certificate revocation; certificates automatically expire after their time or beyond the area. For each new issuance of a certificate the provider checks if a previous certificate for the same user was revoked (the provider needs to maintain a list of all revoked certificates). If a revocation entry exists then new certificate will not be issued. Further, if the certificate is to be revoked before its expiry then RL can be disseminated via roadside units. Since the service is area/time restricted so the RL will be distributed only within the effected area and will contain only the certificates which have still not expired (due to time). This simplifies RL maintenance and distribution.

The system does not require centralized CA or trust relationships among regional CAs. Each provider can work independently

within its coverage area. This minimizes the infrastructure required by a service provider to start its services and will be an incentive for service providers. Initially, a service provider may limit its service within a geographic area and later incrementally extend it. Further, when isolated/widely-separated service areas become adjacent due to the extensions then these can be combined as one region or roaming can be coordinated between the regions. Users and providers both benefit with incremental deployment without paying unnecessarily for the services they do not use or sell. The solution does not require expensive TPDs and periodic refilling of pseudonyms. The user only pays when using the service and does not pay for certificate maintenance.

Payment devices may be operated by a third party and integrated with service providers; one device may be used with different service providers. Further, development of device will be motivated by service providers, who will force security and affordability of the devices. The architecture drives its security from mature Internet payment systems.

As a baseline service, the temporary credentials can be used for all VANET applications including V2V communications. Further, our solution can coexist with other solutions, ensuring smooth transition and unlimited overlapping of the solutions.

4. CONCLUSION

We have presented a distributed certificate architecture that can be incrementally deployed. Users are issued with temporary certificates which can only be used within a specific geographic area and within a particular time period. This property also simplifies the certificate revocation procedure. We have also presented the framework which can be used to provide various services to VANET by providers without investing much in infrastructure. The solution is intended to simulate VANET activity and build user/provider confidence.

5. ACKNOWLEDGMENTS

This work was supported by NSF Cyber Trust Grant CNS-0627318 and Intel Research Fund.

6. REFERENCES

- [1] P. Kamat, A. Baliga, and W. Trappe, An identity based security framework for VANETs, In VANET'06
- [2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J. P. Hubaux, Secure vehicular communication systems: design and architecture, In IEEE Wireless Comm Magazine, Nov 2008
- [3] G. D. Crescenzo, T. Zhang, S. Pietrowicz, Anonymity notions for public-key infrastructures in mobile veh. nets., In MASS'07
- [4] J. Choi and S. Jung, A security framework with strong non-repudiation and privacy in VANETs, In CCNC'09
- [5] F. Armknecht, A. Festag, D. Westhoff, K. Zang, Cross-layer privacy enhancement and non-repudiation in veh. Comm., In WMAN'07
- [6] P. Papadimitratos, G. Mezzour, J. P. Hubaux. Certificate revocation list distribution in vehicular communication systems, In VANET'08
- [7] A. Stampoulis, and Z. Chai, Survey of Security in Vehicular Networks, Project CPSC 534