Refinements to the PAAVE protocol for VANETs

A Kazmierczak
Computer Information Systems
Northwest Arkansas Community College
Bentonville, AR 72712 USA

Abstract - Vehicle ad hoc networks (VANETs) are receiving considerable interest from the research community. One of the concerns in the deployment of such networks is security and privacy. In [1],the authors propose a Protocol for Anonymous Authentication in Vehicular Networks (PAAVE). The protocol provides real-time anonymous authentication between on board units (OBUs) and roadside units (RSUs) via the use of smart cards. The protocol is lightweight and provides fast anonymous authentication between the OBU and the RSU. The protocol does need some refinements from the security perspective. In this paper, we propose such refinements that will make PAAVE a much more secure and reliable protocol.

Keywords: authentication, protocol, security

I INTRODUCTION

With the advances in technology, networks pervade our homes and workplace and now are beginning to work their way into our transportation system. As with any network, there are requirements that must be met to provide a secure networking environment. Vehicular ad hoc networks (VANETs) are being made possible by the Federal Communication Commission (FCC) licensing a range for Dedicated Short Range Radio (DSRC) Service in the Intelligent Transportation (ITS) Radio Service. The standard for VANETs is being developed by the IEEE as IEEE 802.11p [2].

Researches by both industry and academia have already investigated most of the key issues [3, 4, 5]. Some of the primary issues include security related to

Authenticity and integrity of information, vehicle location and misbehaving vehicles is addressed in [4, 6, 7]. With the deployment of vehicular communication via wireless networking, it is particularly easy to eavesdrop on transmissions and collect vehicle-specific information. This could easily lead to the compromise of transmissions and personal information being disclosed to unauthorized parties.

The issue of anonymous message authentication has drawn the interest of researchers [6, 8, 9, 10 11]. Solutions proposed previously either required OBUs to store a very large number of keys [6, 10], or impose very high communication overhead [8, 11] or require very large computational overhead [9, 10]. Thus, the authors in [1] proposed PAAVE to overcome the shortcomings of previous protocols. PAAVE proposes the use of smart cards to preserve confidentiality, integrity and non-repudiation of messages. The advantages of PAAVE include requiring each OBU to store only one key [6, 8], provide minimal communication overhead [9] and minimal message verification time [9].

Unfortunately, the proposed PAAVE protocol does not fully address all security issues at all levels to provide a quality of security that users would find acceptable. In the rest of this paper we address refinements to PAAVE that provide the requisite level of security to make users comfortable with the system.

IIRELATED WORK

The only work that is relevant to our research is the PAAVE protocol [1]. A survey of different types of information and information assurance is covered in [13]. A security architecture is presented in [6] that provides information assurance using hardware and a public key infrastructure for vehicular systems. We do not address the issues related to other protocols such as HAB [6,12], GSB [8, 11], or ECPP [9]. Our only concern is tightening the security of PAAVE. Readers are referred to [1] for details.

IIINETWORK MODEL AND SMART CARDS

A Network Model

There are three components in the PAAVE architecture: a centralized (trusted) agent that issues smart cards and performs key distribution tasks, (trusted) roadside units (RSUs), and the vehicles and their drivers. A VANET is composed of vehicles equipped with onboard units (OBUs) and RSUs. OBUs integrate wireless communications, micro-sensors, embedded systems and Global Positioning Systems (GPS). RSUs and the Trusted Authority (TA) are connected by links that have high bandwidth, low delay, low bit error rates, and, most importantly, highly secure.

B Smart Cards

A smart card is a device, similar to a credit card that contains a microcontroller or a CPUwith internal memory. With an internal CPU, smart cards are able to store data, carry out their own functions (encryption/decryption) and interact with a smart card reader. Smart cards offer physical security and support a variety of authentication techniques, including support for symmetric encryption and asymmetric key services. In [1], the authors mention DES and 3DES encryption algorithms. These two encryption algorithms are no longer acceptable choices. DES has been broken, it took a matter of just a few hours, and 3DES is considered weak encryption. A more secure encryption algorithm needs to be used, like the Advanced Encryption Standard (AES).

IV DESCRIPTION OF THE REFINED PROTOCOL

The first refinement is in the Vehicular Security Model (VSM) which we describe in the next section. In a later section, we describe the entire protocol with refinements.

A Vehicular Security Module (VSM)

The VSM on a smart card stores vehicle identification information, including several required cryptographic keys. We propose that driver's information not be stored on the smart card as this information is unnecessary for protocol operation and exposes the information to potential compromise.

The VSM stores information about the OBUs on the VANET, including OBU_{ID}, $Issuer_{ID}$, public and private keys (K_{PU} and K_{PR}) and the users certificate (V_{CERT}), TA's public key (TA_{PU}), The session key (K_S) and session key identifier (K_{ID}) can be temporarily stored on the card.

- OBU_{ID}: Information that uniquely identifies the OBU, and can be used to identify the vehicle. Any information that uniquely identifies the driver should not be stored on the card.

- $Issuer_{ID}$: Information that identifies the issuer. The issuer must be a trusted entity as this information can be used to verify authenticity and ownership of keys.

- V_{CERT}: The certificate issued by the TA and used to verify ownership of the public/private key pair.

- K_S: The session key issued for secure communication and issued by the RSU
- TA_{PU}: The TA's public key.
- K_{ID}: Session key identifier to identify the key used to encrypt/decrypt messages.

B Refined PAAVE Protocol

All information originating in the OBU is passed to the VSM for encryption. All communication from the RSU is passed through the VSM for decryption. The PAAVE protocol consists of the following components: authentication, session key and message verification.

1) Authentication process

We address only the case where the OBU is in communication range of an RSU. The case where the OBU is not in communication range needs no refinements.

Case 1: An RSU periodically broadcasts a beacon message that contains the RSUs identity and its public key. The RSU should under no circumstances transmit its certificate as the certificate also contains the private key of the RSU. That would completely compromise the security of the system.

Upon hearing a beacon frame, OBU_i transmits a challenge message to verify RSU authenticity:

OBU_i -> RSU: $E_{RSUPU}(E_{KPR}(R_i), OBU_{ID}, Issuer_{ID})$

The OBU also does not transmit its certificate as this certificate holds the private key of the OBU. R_i is a random nonce. The RSU then retrieves the OBUs public key (K_{PU}), which is used to decrypt the nonce. Once the RSU verifies the identity of the OBU, the RSU sends a response message:

$$RSU \rightarrow OBU_i: E_{KPU}(R_i, K_S, T_{exp})$$

The VSM decrypts the message and stores the session key. T_{exp} indicates the session key validity interval.

2) Session Keys for Communication

Each RSU generates a new session key at the beginning of each session after the OBU has been authenticated. The se(H(m) 0ssion key should be unique to each OBU and should never be shared by OBUs, This is a security best practice. If a session key is compromised, it affects every transmission between an OBU and the RSU.

Though OBUs are mobile and move from one RSUs coverage area to another RSUs coverage area, the session key should never be transferred from one RSU to another RSU. When an OBU moves into the coverage area of another RSU, the OBU and the RSU should reauthenticate and the RSU should issue a new session key. Session keys are critical to secure communication and must be changed for each new session.

3) Communication and Message Verification

When the OBU has a message, m, to send, the process needs to be explained in two steps. First, a hash of the message must be generated, H(m), The hash is then encrypted with the OBUs private key to create a digital signature, DS(m).

$$DS(m) \leftarrow E_{KPR}(H(m))$$

The message is then encrypted as:

$$E_{KS}(m, RSU_{PU}(OBU_{ID}), DS(m))$$

The hash H(m) is used to verify the integrity of the message. The digital signature provides non-repudiation, as there is only one entity that can use the OBUs private key to encrypt the hash, the OBU itself.

4) Revocation Lists

Since certificates are subject to being revoked and a revocation list can consume considerable memory, the Certificate Revocation List (CRL) can be kept at each RSU. When an OBU attempts to authenticate to an RSU, the RSU can check its CRL. If the OBUs certificate has been revoked, it may be considered a bad actor and the RSU can fail to authenticate, The CRL needs to be kept at each RSU, this avoids the need to generate extra messages to exchange CRLs and the next RSU will still not authenticate an OBU with a revoked certificate.

V DISCUSSION

The refined PAAVE protocol contains the following security features:

i) When an OBU receives a message, the OBU can be considered authenticated as that is the only way it could have received a session key

ii) Only an OBU that has been authenticated can decrypt a message, thus ensuring confidentiality

iii) An OBU cannot decrypt the digital signature generated by another OBU, thus anonymity is ensured

iv) For message verification, the RSU can decrypt the signature and obtain the transmitting OBUs identity, thus achieving non-repudiation. The RSU can use the hash to verify the integrity

The hallmarks of security are to ensure confidentiality, integrity, availability and non-repudiation. The refined PAAVE protocol achieves confidentiality, integrity and non-repudiation and can thus be considered a very secure protocol.

VIPERFORMANCE

In this paper, we addressed only security issues related to PAAVE. These refinements have no impact on the performance of PAAVE. By comparison to other protocols, PAAVE is still lightweight, fast and even more secure.

VII CONCLUSIONS

The PAAVE protocol for anonymous authentication in VANETs effectively provides such authentication while preserving confidentiality, integrity and non-repudiation. With a strong encryption algorithm and the use of unique session keys, PAAVE can be expected to lead the way in anonymous authentication in VANETs.

5()(5(1&(6#

1. V. Paruchuri, A. Duressi, “PAAVE: Protocol for Anonymous Authentication in Vehicular Networks Using Smart Cards”, Proc. IEEE Globecom, 2010

2. Task Group p, “IEEE 802.11p Wireless Access for Vehicular Environments”, Draft Standard, http://grouper.ieee.org/groups/802/11

3. J. Blum, A. Eskandriant, L. Hoffman, “Challenges of Inter-Vehicle Ad Hoc Networks”, IEEE Transactions on Intelligent Transportation Systems, Vol 5, No 4, pp347-351

4. F. Kargi, P. Papadimitratos, L. Buttyan, M. Mueter, E. Schoch, B. Weidersheim, T-V, Thong, G. Calandriello, A. Held, A. Kang, J-P. Hubaux, “Secure Vehicular Communication Systems: Implementation, Performance and Research Challenges”, IEEE Communications Magazine, Vol 46, No 11, Nov 2008

5. J. Rybicki, B. Scheuermann, W, Keiss, C. Lochert, P. Fallah, M. Mauve, “Challenge: Peer on Wheels – A Road to New Traffic Information Systems”, ACM Proc of MobiCom, Sep 2007

6. M. Raya, J-P Hubaux, “Securing Vehicular Ad Hoc Networks”, Journal of Computer Security, Vol 15, No 1, pp. 39-68, 2007

7. B. Parma, A. Perring, Challenges in Securing Vehicular Networks”, Proc of HotNets-IV, 2005

8. X. Liu, X. Sun, P-H. Ho, X. Shen, “GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications” IEEE Transactions on Vehicular Technology”, Vol 56, No 6, pp. 3442-3456, 2007

9. R. Lu, X. Lin, H. Zhu, P-H Ho, X. Shen, “ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications”, Proc IEEE Infocom, 2008

10. X. Lin, X. Sun, X. Wang, C. Zhang, P-H Ho, X. Shen, “TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving” IEEE Transactions on Wireless Communications, 2008

11. A. Wasef, X. Shen, “PPGCV: Privacy Preserving Group Communication Protocol for Vehicular Ad Hoc Networks”, Proc IEEE ICC’08, Beijing, China, May 2008

12. G. Caladriello, P. Papadimitratos, J-P. Hubaux, “Efficient and Robust Pseudonymous Authentication in VANET”, Proc ACM Workshop on Vehicular Ad Hoc Networks, Sep 2007

13. P. Krishmamurty, “Information Dissemination and Information Assurance in Vehicular Networks: A Survey”, Proc iConference’08, Los Angeles, Feb 2008

$°–ª ƚß¹#øßƚ–Ŀ°ˇ#

Dr. Kazmierczak received his PhD in Computer Science from the University of Oklahoma in 1993. He is currently teaching Computer Information Systems at a local community college.