The Security of VANETs

Maxim Raya and Jean-Pierre Hubaux
Laboratory for computer Communications and Applications (LCA)
School of Computer and Communication Sciences
EPFL, Switzerland
maxim.raya@epfl.ch, jean-pierre.hubaux@epfl.ch

ABSTRACT

In this work, we address the security of VANETs. We provide a detailed threat analysis and devise an appropriate security architecture. We also describe some major design decisions still to be made, which in some cases have more than mere technical implications. We provide a set of security protocols, we show that they protect privacy and we analyze their robustness, and we carry out a quantitative assessment of the proposed solution.

Categories and Subject Descriptors: C.2.0 [Computer-Communication Networks]: General—Security and protection

General Terms: Design, Security

Keywords: vehicular networks, security

1. INTRODUCTION

Until recently, road vehicles were the realm of mechanical engineers. But with the plummeting costs of electronic components and the permanent willingness of the manufacturers to increase road safety and to differentiate themselves from their competitors, vehicles are becoming "computers on wheels", or rather "computer networks on wheels". Manufacturers are about to make a quantum step in terms of vehicular IT, by letting vehicles communicate with each other and with roadside infrastructure; in this way, vehicles will dramatically increase their *awareness* of their environment, thereby increasing safety and optimizing traffic. Considering the tremendous benefits expected from vehicular communications and the huge number of vehicles (hundreds of millions worldwide), it is clear that vehicular communications are likely to become the most relevant realization of mobile ad hoc networks. The appropriate integration of on-board computers and positioning devices such as GPS receivers, along with communication capabilities, open tremendous business opportunities, but also raise formidable research challenges. One of these challenges is security; limited attention has been devoted so far to the security of vehicular networks [1, 2, 4]. Yet, security is crucial. It is essential to make sure that life-critical information cannot be inserted or modified by an attacker; likewise, the system should be able to help establish the liability of drivers; but it should also protect the privacy of the drivers and passengers.

Copyright is held by the author/owner.
VANET'05, September 2, 2005, Cologne, Germany.
ACM 1-59593-141-4/05/0009.

2. ATTACKS ON VANETS

We focus on the security aspects of safety-related applications, such as collision avoidance and cooperative driving. We have identified several attacks on the safety messages: *Bogus information*, *Cheating with positioning information*, *ID disclosure* of other vehicles in order to track their location, *Denial of Service*, and *Masquerade*. The attacker can be *Insider/Outsider*, *Malicious/Rational*, *Active/Passive*. Detailed descriptions of the attacks and the attacker model can be found in [3].

3. HOW TO SECURE VANETS

A security system for safety messaging in a VANET should satisfy the following requirements to be able to thwart any generic attack on vehicular networks:*Authentication*, *Verification of data consistency*, *Availability*, *Non-repudiation*, *Privacy*, and *Real-time constraints*.

Digital signatures are a better choice than symmetric authentication mechanisms in the VANET setting, because safety messages should be sent to receivers as fast as possible. In fact, a preliminary handshake is not acceptable and actually creates more overhead. In addition, given the huge amount of network members and the sporadic connectivity to authentication servers, a PKI (Public Key Infrastructure) is the most suitable way for implementing authentication (in [3], we provide performance evaluation of different Public Key Cryptosystems and show that some of them are suitable for VANETs). Under the PKI solution, each vehicle will be assigned a public/private key pair. Before a vehicle sends a safety message, it signs it with its private key and includes the CA's (Certification Authority) certificate as follows (T is the timestamp):

$$V \rightarrow * : M, Sig_{PrK_V}[M|T], Cert_V$$

The receivers of the message have to extract and verify the public key of V using the certificate and then verify V's signature using its certified public key. In order to do this, the receiver should have the public key of the CA, which can be preloaded as described below. If the message is sent in an emergency context, this message should be stored (including the signature and the certificate) in the EDR (Event Data Recorder, reminiscent of the "black boxes" used in avionics) for further potential investigations about the emergency.

The use of secret information such as private keys incurs the need for a tamper-proof device in each vehicle. In addition to storing the secret information, this device will be also responsible for signing outgoing messages.

3.1 Key management

To be part of a VANET, each vehicle has to store the following cryptographic information:

1. An electronic identity called an *Electronic License Plate* (*ELP*) if issued by the government, or alternatively an *Electronic Chassis Number* (*ECN*) if issued by the vehicle manufacturer. These identities should be unique and cryptographically verifiable. The governmental transportation authority will preload the ELP at the time of vehicle registration (in the case of the ECN, the manufacturer is responsible for its installation at production time).

2. *Anonymous key pairs* that are used to preserve privacy. An *anonymous key pair* is a public/private key pair that is authenticated by the CA but contains no information about the actual identity of the vehicle (i.e., its ELP). Yet this anonymity is conditional for liability purposes. Normally, a vehicle will possess a large set of anonymous keys to prevent tracking. Anonymous keys are preloaded by the transportation authority or the manufacturer and periodically renewed.

Certification Authorities (CA) will be responsible for issuing key certificates to vehicles. Two solutions can be envisioned:

1. *Governmental transportation authorities*: Vehicles will be registered in different countries by the corresponding transportation authorities (which are usually regional). The advantage of this option is that the certification procedure will be under the direct control of the concerned authority.

2. *Vehicle manufacturers*: Certificates can also be issued by vehicle manufacturers, given their limited number and the trust already endowed in them. The advantage of this approach is reduced overhead.

We consider two key revocation scenarios depending on the information compromised by the attacker:

1. All the cryptographic material belonging to a vehicle is compromised. To avoid the overhead of revoking all the keys of this vehicle, the CA will revoke them by sending secure revocation messages to the tamper-proof device.

2. A particular key of a vehicle's key set is compromised. In this case, sending a revocation message to the tamper-proof device for each revoked key would cause a large overhead. We opt for using *short key certificate lifetimes* that will make key certificates expire, thus revoking the keys.

3.2 Verification by correlation

In the *bogus information* attack, one or several legitimate members of the network send out false information to misguide other vehicles about traffic conditions. To thwart such misbehavior, data received from a given source should be verified by correlating them with those received from other sources. This is typically done by reputation-based systems. It is important to stress here that what matters is the rating of the correctness of the data rather than its source.

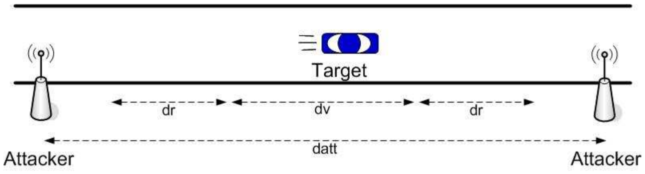

Figure 1: *ID disclosure* attack.

3.3 Anonymity

In order to preserve the driver's anonymity and minimize the storage costs of public keys, we propose a key changing algorithm that adapts to the vehicle speed and takes into account key correlation by the attacker. Let us consider the typical tracking scenario where the attacker controls stationary base stations separated by a distance d_{att} and captures all the received safety messages. Assume the speed of target V is v_t, its transmission range is d_r, and d_v is the distance over which a vehicle does not change its speed and lane (the vulnerability window with respect to the correlation of identifiers, including keys, by an attacker). As Fig. 1 illustrates, the vehicle's anonymity is vulnerable over a distance equal to $d_v + 2d_r$. This means that it is not worth changing the key over smaller distances because an observer can correlate keys with high probability. This defines the lower bound on the key changing interval T_{key}:

$$min(T_{key}) = \frac{d_v + 2d_r}{v_t} \text{ seconds} \quad (1)$$

But if $d_{att} > d_v + 2d_r$, V can avoid being tracked (by changing its key) as long as it does not use the same key for a distance equal to or longer than d_{att}. This in turn defines the upper bound on the key changing interval:

$$max(T_{key}) = \frac{d_{att}}{v_t} \text{ seconds} \quad (2)$$

Since V does not know d_{att}, but knows d_r and d_v, it can choose a value of T_{key} that is a little larger than $min(T_{key})$. If we denote by r_m the message sending rate for V, one key should be used for:

$$N_{msg} = \lceil r_m \times T_{key} \rceil \text{ messages} \quad (3)$$

4. CONCLUSION

In this work, we have explained why vehicular networks need to be secured, and why this problem requires a specific approach. We have also identified the major threats. We have then proposed a security architecture along with the related protocols; we have shown how and to what extent it protects privacy. In terms of future work, we intend to further develop this proposal and perform additional numerical evaluations of the solutions.

5. REFERENCES

[1] http://ivc.epfl.ch/

[2] J. Blum and A. Eskandarian, "The threat of intelligent collisions," *IT Professional*, 6(1):24-29, Jan.-Feb. 2004.

[3] M. Raya and J.P. Hubaux, "The Security of Vehicular Networks," *EPFL Technical report*, 2005.

[4] M. El Zarki, S. Mehrotra, G. Tsudik and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network," *European Wireless*, 2002.