The UNESCO Chair in Data Privacy Research in Vehicular Networks

Josep Domingo-Ferrer

Universitat Rovira i Virgili,
UNESCO Chair in Data Privacy,
Dept. of Computer Engineering and Mathematics,
Av. Països Catalans 26, E-43007 Tarragona, Catalonia
josep.domingo@urv.cat

Abstract. An overview of the activities of the UNESCO Chair in Data Privacy is first given. One of these activities is research. We focus on the research conducted to conciliate security and privacy in vehicular ad hoc networks (VANETs) and, specifically, in VANET announcements.

Keywords: Vehicular *ad hoc* networks, Privacy, Trust, Car-to-car messages.

1 Introduction

The UNESCO Chair in Data Privacy (http://unescoprivacychair.urv.cat) is an agreement between UNESCO and Universitat Rovira i Virgili, who acts as a host institution for the Chair. The agreement was signed on March 6, 2007, and it is renewed every two years by mutual consent. A UNESCO Chair must do research, cooperation, training and dissemination in a field considered relevant by UNESCO for the welfare of humankind; in the case of the Chair in Data Privacy, the focus is on privacy, already mentioned as a fundamental right in Article 12 of the Universal Declaration of Human Rights (1948):

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Beyond the host institution, there are participating institutions in the UNESCO Chair in Data Privacy including, among others, the United Nations Economic Commission for Europe (UN/ECE), CSIC (Spain's Higher Council for Scientific Research), Sabanci University (Istanbul, Turkey), Destatis-Statistisches Bundesamt (Germany) and CBS-Statistics Netherlands.

The most visible actions by the Chair include:

Dissemination: Organization of the biennial *Privacy in Statistical Databases-PSD* conference, with LNCS proceedings (Barcelona, 2004, LNCS 3050;

J. Garcia-Alfaro et al. (Eds.): DPM 2009 and SETOP 2009, LNCS 5939, pp. 1–8, 2010.

Rome, 2006, LNCS 4302; Istanbul, 2008, LNCS 5262; Corfu, 2010) and publication of the *Transactions on Data Privacy* journal (TDP, `http://www.tdp.cat`). TDP is jointly published with IIIA-CSIC and it is currently indexed by DBLP, ACM Digital Library, MathScinet and DOAJ.

Co-operation: The Chair regularly sponsors a number of privacy research conferences by offering travel grants for authors and attendees from transition countries.

Research Researchers from the Chair co-ordinate several research projects on creating new information technologies that conciliate privacy, security and technology. The most revelant of those is the CONSOLIDER INGENIO 2010 project "ARES" (`http://crises-deim.urv.cat/ares`), a five-year endeavor (2007-2012) co-ordinated by this author and involving a multinational team of about 80 researchers from six different universities.

In the rest of this talk, we focus on a specific research scenario where we are particularly active at the Chair's host institution (URV): vehicular *ad hoc* networks (VANETs). It will be argued that VANETs are especially challenging in what regards the combination of privacy, security and functionality. Section 2 introduces VANETs. Section 3 reviews the countermeasures proposed in the literature to obtain secure and privacy-preserving VANETs. Section 4 discusses how to combine *a priori* and *a posteriori* countermeasures in order to overcome the shortcomings of proposals in the literature. Section 5 is a conclusion.

2 Vehicular *Ad Hoc* Networks

According to recent technology forecasts [1], vehicles will be equipped with radio interfaces in the near future and vehicle-to-vehicle (V2V) communications will be available in vehicles by 2011. The IEEE 802.11p task group is working on the Dedicated Short Range Communications (DSRC) standard which aims at enhancing the 802.11 protocol to support wireless data communications for vehicles and the road-side infrastructure [19]. Car manufacturers and telecommunication industry gear up to equip each car with devices known as On-Board Units (OBUs) that allow vehicles to communicate with each other, as well as to supply Road-Side Units (RSUs) to improve safety, traffic efficiency, driver assistance, and transportation regulation. The RSUs are expected to be located at the critical points of the road, such as traffic lights at road intersections. The OBUs and RSUs form a self-organized network called a VANET, emerging as the first commercial instantiation of the mobile *ad hoc* networking (MANET) technology.

VANETs allow nodes including vehicles or road-side infrastructure units to communicate with each other over single or multiple hops. In other words, nodes will act both as end points and routers. Vehicular networking protocols allow vehicles to broadcast messages to other vehicles in the vicinity. It is suggested that each vehicle periodically send messages over a single hop every 300ms within a distance of 10s travel time (which means a distance range between 10m and 300m)[17]. This mechanism can be used to improve safety and optimize traffic.

However, malicious vehicles can also make use of this mechanism by sending fraudulent messages for their own profit or just to jeopardize the traffic system. Hence, the system must be designed to ensure that the transmission comes from a trusted source and has not been tampered with since transmission.

Another critical concern in VANETs is the privacy or anonymity of the driver (or the vehicle, for that matter). As noted in [6], a lot can be inferred about the driver if the whereabouts and the driving pattern of a car can be tracked. It is indeed possible for attackers to trace vehicles by using cameras or physical tracking, but such physical attacks can only trace specific targets and are much more expensive than monitoring the communication in VANETs. Hence, most studies focus on thwarting the latter attacks.

3 Countermeasures for Securing VANETs

VANETs can improve traffic safety only if the messages sent by vehicles are trustworthy. Dealing with fraudulent messages is a thorny issue for safety engineers due to the self-organized operation of VANETs. The situation is further deteriorated by the privacy requirements of vehicles since, in a privacy-preserving setting, the message generators, *i.e.* the vehicles, are anonymous and cannot be identified when acting maliciously. A number of schemes have been proposed to reduce fraudulent messages; such proposals fall into two classes, namely *a posteriori* and *a priori*.

3.1 *A Posteriori* Countermeasures

A posteriori countermeasures consist in taking punitive action against vehicles which have been proven to have originated fraudulent messages. To be compatible with privacy preservation, these countermeasures require the presence of a trusted third party able to open the identities of dishonest vehicles. Then the identified vehicles can be removed from the system.

Cryptographic authentication technologies have been extensively exploited to offer *a posteriori* countermeasures. Most proposals use regular digital signatures and require a public-key infrastructure. See [5] for a survey.

A critical issue posed by vehicular message authentication is driver's privacy. Since the public key used to verify the authenticated messages can be linked to specific users, attackers can trace vehicles by observing vehicular communications. Hence, mechanisms must be adopted to guarantee vehicle/driver privacy when vehicles authenticate messages. Along this research line, there are two main approaches: pseudonymous mechanisms and group signatures.

In a pseudonymous mechanism, the certificate authorities produce multiple pseudonyms for each vehicle so that attackers cannot trace the vehicles producing signatures in different periods under different pseudonyms, except if the certificate authorities open the identities of the vehicles. Pseudonymous mechanisms have been extensively investigated from various aspects. Short-lived certificates are also suggested in [11], mainly from the perspective of how often a

node should change a pseudonym and with whom it should communicate. The authors of [18] propose to use a silent period in order to hamper linkability between pseudonyms, or alternatively to create groups of vehicles and restrict vehicles in one group from hearing messages of other groups.

This conditional anonymity of pseudonymous authentication will help determining the liability of drivers in the case of accidents. The downside of this approach is the necessity for generation, delivery, storage, and verification of numerous certificates for all the keys. To mitigate this heavy overhead, [2] presents an approach to enable vehicle on-board units to generate their own pseudonyms without interacting with the CAs. The mechanism is realized with the help of group signatures. In [10] a novel group signature-based security framework is proposed which relies on tamper-resistant devices (requiring password access) for preventing adversarial attacks on vehicular networks. However, they provide no concrete instantiation or experiment analysis.

In [12], the authors propose a secure and privacy-preserving protocol for VANETs by integrating the techniques of group signature and identity-based signature. In their proposal, they take into account security and privacy preservation between OBUs, as well as between OBUs and RSUs. In the former aspect, a group signature is employed to secure the communication between OBUs, where messages are anonymously signed by the senders while the identities of the senders can be traced by the trusted authorities if the messages are later found to be doubtable. In the latter aspect, an identity-based signature scheme is used at RSUs to sign each message generated by RSUs to ensure its authenticity. With their approach, the heavy load of certificate management can be greatly reduced.

3.2 *A Priori* Countermeasures

VANETs can improve traffic safety and efficiency only if vehicular messages are correct and precise. Despite the security provided by the combination of TPDs with authenticated messages, an attacker could still manage to transmit valid messages containing false data. It is easy for an attacker to launch such an attack. For instance, putting the vehicle temperature sensor in cold water will let the OBUs generate false messages, even if the hardware sensors are tamper-proof. Also, one may note that in some cases the sender of the data may not necessarily be malicious, but his vehicle's sensors may be out of order. To rule out such cases of false data, one needs not only to verify that the sender of the data is legitimate, but also that the data are correct. Therefore some mechanisms for detection of malicious data need to be explored. We refer to such approaches as *a priori* countermeasures which attempt to prevent the generation of erroneous messages in advance.

A detailed survey on *a priori* countermeasures can be found in [5]. Here we will mention only the most efficient class, namely threshold-based mechanisms [8,14,15,16,4]. In these proposals, a message is trusted only if it was endorsed by a number of vehicles in the vicinity. This approach is based on the assumption that most users are honest and will not endorse any message containing false

data. Another implicit assumption is the usual common sense that, the more people endorse a message, the more trustworthy it is. Among these schemes, the proposals in [4] may be the most efficient while enabling anonymity of message originators by exploiting secret sharing techniques. But their scheme does not provide anonymity revocability, which may not suit some applications in which anonymity must be revoked "for the prevention, investigation, detection and prosecution of serious criminal offences"[7].

3.3 Discussion on Existing Countermeasures

Unfortunately, neither *a posteriori* nor *a priori* countermeasures suffice on their own to secure VANETs. By taking strict punitive action, *a posteriori* countermeasures can protect against rational attackers producing bogus messages to obtain benefits or pranks. However, they are ineffective against irrational attackers such as terrorists. Even for rational attackers, damage has already occurred when punitive action is taken. It seems that *a priori* countermeasures function better in this case because they prevent damage beforehand by letting the vehicles trust only messages endorsed by a certain number of vehicles. However, although the underlying assumption that there is a majority of honest vehicles in VANETs generally holds, it cannot be guaranteed that a number of malicious vehicles greater than or equal to the threshold will never be present at specific locations. For example, this is likely to happen if some criminal organization undertakes to divert traffic from a certain area by broadcasting messages informing that a road is barred. Furthermore, for convenience of implementation, existing schemes use an even stronger assumption that the number of honest vehicles in all cases should be at least a preset threshold. But such a universally valid threshold does not exist in practice. Indeed, the threshold should somehow take the traffic density and the message scope into account: a low density of vehicles calls for a lower threshold, whereas a high density and a message relevant to the entire traffic of a city requires a sufficiently high threshold.

The situation is aggravated by the anonymity technologies used in some proposals. A system preserves anonymity when it does not require the identity of its users to be disclosed. Without anonymity, attackers can trace all the vehicles by monitoring the communication in VANETs, which in turn can enable the attackers to mount serious attacks against specific targets. Hence, anonymity is a critical concern in VANETs. However, anonymity can also weaken *a posteriori* and *a priori* countermeasures. Indeed, attackers can send fraudulent messages without fear of being caught, due to anonymity; as a result, no punitive action can be taken against them. Furthermore, some proposals provide strong anonymity, *i.e.* unlinkability. Unlinkability implies that a verifier cannot distinguish whether two signatures come from the same vehicle or two vehicles. This feature may enable malicious vehicles to mount the so-called Sybil attack: a vehicle generates a fraudulent message and then endorses the message herself by computing on it as many signatures as required by the threshold in use; since signatures are unlinkable, no one can find out that all of them come from the same vehicle. Hence, elegantly designed protocols are required to secure VANETs

when incorporating anonymity. It must be noted that, among those threshold-based systems cited above which provide *a priori* protection and anonymity, [4] is the only one resistant to the Sybil attack: in that system, vehicles belong to groups, and vehicles in a group share keys (which provides vehicle anonymity because vehicles in a group are interchangeable as far as signing goes); however, for a message to be validated, endorsements from a number of different groups are needed, so a single vehicle cannot get a message sufficiently endorsed.

4 Towards a Combination of *a Priori* and *a Posteriori* Countermeasures

Our focus is to devise a context-aware threshold authentication framework with conditional privacy in VANETs, equipped with the following properties: i) it should be privacy-preserving; ii) it should support an adaptive threshold authentication mechanism (*a priori* security); iii) it should allow anonymity revocation in case of offence (*a posteriori* security).

4.1 Message-Linkable Group Signatures

Group signatures have been investigated for many years [3,9]. In a group signature scheme, each group member can anonymously sign messages on behalf of the group. However, a group manager can open the identity of the author of any group signature in case of dispute. Most existing group signatures provide unlinkability in the sense that no efficient algorithm can tell whether two group signatures are generated by the same group member, even if the two signatures are on the same message. Linkable group signatures [13] are a variant of group signatures. In a linkable group signature, it is easy to identify the group signatures produced by an identical signer, even if the signer is anonymous. This feature is desirable in e-voting systems where each voter can anonymously vote only once.

Group signatures are useful for securing VANETs but they are vulnerable to the Sybil attack because of unlinkability. Linkable group signatures can thwart the Sybil attack but are not compatible with vehicle privacy due to the linkability of signer identities, *i.e.* the various message endorsements signed by a certain vehicle can be linked. Hence, a more sophisticated notion of linkability is required in group signatures for VANETs. Motivated by this observation, we presented in [5,20] a new primitive referred to as message-linkable group signatures (MLGS).

An MLGS scheme has the same security properties as regular group signatures except that, given two signatures on *the same message*, one can easily decide whether the two signatures are generated by the same member or by two different members, but the originator(s) stay(s) anonymous.

4.2 A New Solution Based on Message-Linkable Group Signatures

Based on MLGS, we propose a general framework for threshold authentication with revocable anonymity in VANETs. In this framework, each vehicle registers

to a vehicle administration office serving as a group registration manager. When t vehicles wish to endorse some message, they can independently generate an MLGS signature on that message. After validating t MLGS signatures on the message, the verifying vehicle is convinced by the authenticated message. However, if later the message is found incorrect, the police office as well as judges (serving as the tracing manager) can trace the t cheating signers. Here, we assume that an honest signer never needs to sign the same message twice. This assumption is workable by embedding a time-stamp in each message, as suggested in most authentication schemes for VANETs, if the OBU of a vehicle senses the same situation at different times.

From the security properties of MLGS schemes, it is clear that the above framework satisfies the required properties of privacy preservation, as well as *a priori* and *a posteriori* security. If $t-1$ vehicles produce t signatures on the same message, then there exists a group member who has been involved in generating at least two signatures. Such an impersonation can be easily identified since the MLGS scheme is message-linkable. Furthermore, the resulting scheme is highly efficient, as required in VANETs. See [20] for more details.

5 Conclusions

We have presented the activities of the UNESCO Chair in Data Privacy and we have sketched the state of the art and the Chair research as regards security and privacy in vehicular networks.

Acknowledgments and Disclaimer

This work was partly supported by the Spanish Government through projects CONSOLIDER INGENIO 2010 CSD2007-0004 "ARES" and TSI2007-65406-C03-01 "E-AEGIS", and by the Government of Catalonia under 2009 SGR 1135. The author is partly supported as an ICREA-Acadèmia researcher by the Government of Catalonia. He is with the UNESCO Chair in Data Privacy, but his views do not necessarily reflect the position of UNESCO nor commit that organization.

References

1. Blau, J.: Car talk. IEEE Spectrum 45(10), 16 (2008)
2. Calandriello, G., Papadimitratos, P., Lioy, A., Hubaux, J.-P.: Efficient and robust pseudonymous authentication in VANET. In: Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks-VANET 2007, pp. 19–28 (2007)
3. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
4. Daza, V., Domingo-Ferrer, J., Sebe, F., Viejo, A.: Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology 58(4), 1876–1886 (2009)

5. Domingo-Ferrer, J., Wu, Q.: Safety and privacy in vehicular communications. In: Bettini, C., Jajodia, S., Samarati, P., Wang, S. (eds.) Privacy in Location-Based Applications, ch. 3, Springer, Heidelberg (to appear, 2009)
6. Dötzer, F.: Privacy issues in vehicular ad hoc networks. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 197–209. Springer, Heidelberg (2006)
7. European Parliament. Legislative resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 C6-0293/2005 2005/0182(COD)) (2005)
8. Golle, P., Greene, D., Staddon, J.: Detecting and correcting malicious data in VANETs. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, pp. 29–37 (2004)
9. Groth, J.: Fully anonymous group signatures without random oracles. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 164–180. Springer, Heidelberg (2007)
10. Guo, J., Baugh, J.P., Wang, S.: A group signature based secure and privacy-preserving vehicular communication framework. In: Mobile Networking for Vehicular Environments, pp. 103–108 (2007)
11. Jakobsson, M., Wetzel, S.: Efficient attribute authentication with applications to ad hoc networks. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks - VANET 2004 (2004)
12. Lin, X., Sun, X., Ho, P.-H., Shen, X.: GSIS: A secure and privacy preserving protocol for vehicular communications. IEEE Transactions on Vehicular Technology 56(6), 3442–3456 (2007)
13. Nakanishi, T., Fujiwara, T., Watanabe, H.: A linkable group signature and its application to secret voting. Transactions of Information Processing Society of Japan 40(7), 3085–3096 (1999)
14. Ostermaier, B., Dötzer, F., Strassberger, M.: Enhancing the security of local danger warnings in VANETs - A simulative analysis of voting schemes. In: Proceedings of the Second International Conference on Availability, Reliability and Security, pp. 422–431 (2007)
15. Parno, B., Perrig, A.: Challenges in securing vehicular networks. In: Proceedings of the ACM Workshop on Hot Topics in Networks (2005)
16. Raya, M., Aziz, A., Hubaux, J.-P.: Efficient secure aggregation in VANETs. In: Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks - VANET 2006, pp. 67–75 (2006)
17. Raya, M., Hubaux, J.-P.: The security of vehicular ad hoc networks. In: 3rd ACM Workshop on Security of Ad hoc and Sensor Networks-SASN 2005, pp. 11–21 (2005)
18. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., Sezaki, K.: CARAVAN: Providing Location Privacy for VANET. Proc. of ESCAR 2005 (November 2005)
19. U.S. Department of Transportation, National Highway Traffic Safety Administration, Vehicle Safety Communications Project, Final Report (April 2006), `http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFTOC.htm`
20. Wu, Q., Domingo-Ferrer, J., González-Nicolás, Ú.: Balanced trustworthiness, safety and privacy in vehicle-to-vehicle Communications (Manuscript under review) (2009)