The UNESCO Chair in Data Privacy Research in Vehicular Networks

Josep Domingo-Ferrer

Universitat Rovira i Virgili

UNESCO

Chair in Data Priv@cy

SETOP 2009/DPM 2009, Saint-Malo

September 24, 2009

UNESCO Chair in Data Privacy Motivation (I)

- Data privacy is the adaptation to the Information Society of the fundamental right to privacy and private life, included by the United Nations in the Universal Declaration of Human Rights (1948), whose Article 12 states:

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

UNESCO Chair in Data Privacy Motivation (II)

- Data privacy technologies are about technically enforcing the above right in the information society
- The design of such privacy technologies requires high-level information protection expertise, which is lacking in transition countries and even in many developed countries due to:
  - Lack of awareness of the population on the existing privacy threats (profiling,location tracking, etc.)
  - Lack of pressure on the service and technology providers
  - Lack of private investment in the development of privacy-preserving technologies

UNESCO Chair in Data Privacy Motivation (III)

- Unless direct action is taken, the spread of the information society might result in serious privacy loss, especially in rapidly developing countries
- The lack of privacy undermines most of all other fundamental rights (freedom of speech, democracy, etc.)

What is the UNESCO Chair?

- It is an agreement between UNESCO and an academic institution (Universitat Rovira i Virgili) for a renewable period of two years time (starting Mar. 6, 2007)
- It must do research, training and dissemination in a field considered relevant by UNESCO for the welfare of humankind (data privacy)
- It is not directly funded by UNESCO, but by whatever funds the UNESCO umbrella can help raise (*e.g.* URV, Government of Catalonia, etc.)
- It can have associated participating institutions

Participating institutions

- **URV**: Rovira i Virgili University. Host institution. Faculties of Engineering and Law.
- **UN/ECE**: Statistical Division of the U.N. Economic Comission for Europe
- **CSIC**: Spanish Higher Research Council
- **Sabanci**: Sabanci University, Istanbul, Turkey
- **Destatis:** Statistisches Bundesamt (Germany)
- **CBS**: Statistics Netherlands
- **INE**: Statistics Spain
- **INSSE**: Statistics Romania
- **NSI**: Statistics Bulgaria
- …

Dissemination

- Organization of the biennial **Privacy in Statistical Databases - PSD conference**, with LNCS proceedings (Barcelona, 2004, LNCS 3050; Rome, 2006, LNCS 4302; Istanbul, 2008, LNCS 5262; Corfu, 2010)
- 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 Josep Domingo-Ferrer
  - Involving a multinational team of about 80 researchers from six different universities.

UNESCO Chair & VANETS

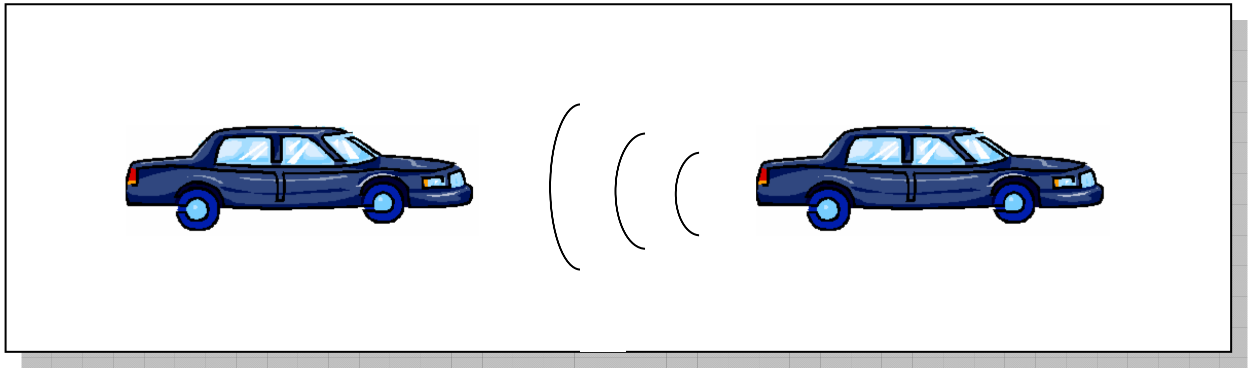
- VANETS: Vehicular Ad-hoc NETworks
- Specific research scenario particularly active at the Chair’s host institution (URV)
- VANETs are emerging as the first commercial instantiation of MANETs
- Intriguing combination of privacy, security and functionality

VANETs – Introduction (I)

- 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)
  - It supports wireless data communications for vehicles and roadside infrastructure
- Car manufacturers and telecommunication industries gear up to equip each car with devices known as On-Board Units (OBUs)
  - They allow vehicles to communicate with each other
- VANETs allow vehicles to disseminate messages about road conditions to other vehicles

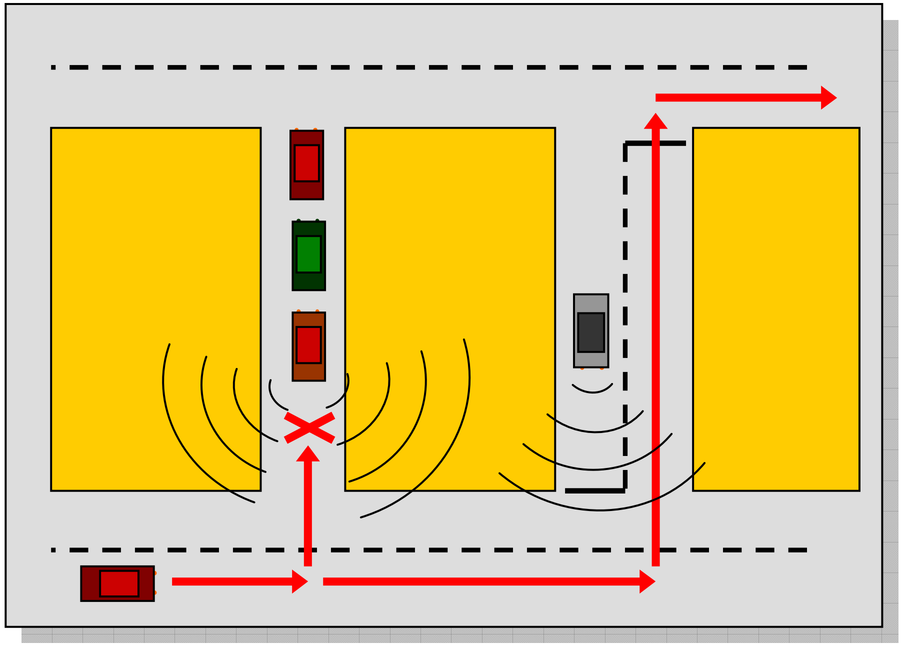
VANETs – Introduction (II)

- Alert messages
  - They warn about dangerous actions like braking
  - Limited range of dissemination
  - Hard real-time requirements
  - Accident prevention



VANETs – Introduction (III)

- Announcement messages
  - They inform about relevant traffic conditions
    - Traffic jams, accidents
  - Broad range of dissemination
  - Slack real-time requirements
  - They facilitate the choice of alternative routes to avoid conflicting places



VANETs – Introduction (IV)

- The motivation of VANETs is to improve
  - Public safety
  - Traffic efficiency
  - Driver assistance
  - Transportation regulation
- Preconditions are
  - Message from vehicles are trustworthy
  - Vehicles are cooperative
  - There are no malicious deviations

VANETs – Introduction (V)

- Architecture of VANETs
  - Semi-trusted (or trusted) electronic administration authorities for
    - Vehicle manufacturers
    - Transportation regulation offices
    - Traffic police and judges
  - Distributed authorities
    - Roadside units (RSUs). Assistance for administration, communication, information collection.
  - Mobile units
    - OBUs embedded in vehicles
  - Communication channels among entities

VANETs – Introduction (VI)

- Operational features of VANETs
    - Nodes move very fast at high relative speeds
    - The duration of the connection among mobile nodes may be very short
    - The number of mobile nodes in VANETs is extremely large.
    - Vehicles must verify a large number of message-signature pairs per time unit
    - Vehicles can be expected to have substantial computational capacity, storage space and power supply

Security concerns in VANETs (I)

- Safety concerns
  - Message trustworthiness can be compromised
    - False messages can be produced
    - Impersonation can be used to inject false messages
    - Messages can be tampered with
    - Denial of service by message flooding (not considered here)
- Privacy concerns
  - Location and identity privacy
    - Driving profile
    - Location profile
    - Location and identity linkage

Security concerns in VANETs (II)

- Attackers
  - Insider attacks vs outsider attacks
    - Insider attacks: attacker is a registered entity
    - Outsider attacks: attacker is not registered
  - Rational attacks vs irrational attacks
    - Rational attacks: cost<benefit
    - Irrational attacks: achieve goal at any cost
  - Electronic attacks vs physical attacks
    - Electronic attacks: by message generation, tampering, information collection, data mining, impersonation, etc
    - Physical attacks: physical tracing, camera or video recording (not considered here)

Countermeasures for securing VANETs (I)

- 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
- A number of schemes have been proposed to reduce fraudulent messages
  - *A posteriori:* Punitive action against vehicles who have been proven to have originated fraudulent messages
  - *A priori:* Prevent the generation of fraudulent messages

Countermeasures for securing VANETs (II)

- *A posteriori* countermeasures
  - Identify malicious vehicles are required
  - Privacy preservation
    - Require the presence of a trusted third party able to open the identities of dishonest vehicle

Countermeasures for securing VANETs (III)

- *A posteriori* countermeasures
  - Cryptographic authentication technologies
    - Based on regular digital signatures:
      - An efficient algorithm generates public-private key pairs
      - Public key is certified by Certification Authorities (CAs)
      - Public keys are bound to vehicles and can be viewed as identities
      - The public key can be used to verify signatures
      - The private key is known only by the owner
      - The private key can be used to generate signatures on any message
      - The attacker cannot generate valid signatures without the private key

Countermeasures for securing VANETs (IV)

- *A posteriori* countermeasures
  - Cryptographic authentication technologies
    - Based on regular digital signatures [RPH06], [RH07], [RPAJ07], [AFWZ07]
      - Only messages endorsed by vehicles are trusted
      - Messages are endorsed with signatures
      - Privacy is provided by a pseudonym mechanism
      - Certificate authorities (CAs) certify several pseudonyms for each vehicle
      - Only CAs can trace identities of vehicles
      - Vehicles producing fraudulent messages can be punished

Countermeasures for securing VANETs (V)

- *A posteriori* countermeasures
  - Cryptographic authentication technologies
    - Based on group signatures [GBW07]
      - Only messages endorsed by vehicles are trusted
      - Messages are endorsed with group signatures
      - Privacy provided by the anonymity of group signatures
      - Group manager can trace the identities of vehicles
      - Vehicles producing fraudulent messages can be punished

Countermeasures for securing VANETs (VI)

- *A posteriori* countermeasures
  - Cryptographic authentication technologies
    - Based on ring signatures
      - No need of trusted group manager
      - Each vehicle has a public-private key pair
      - Public keys are certified by CA
      - Vehicles can form a group on the fly (Good property for VANETs)
      - Any and only group members can generate ring signatures on behalf of the group
      - Signers are anonymous
      - Anonymity cannot be revoked (Not so good property for VANETs)

Countermeasures for securing VANETs (VII)

- *A posteriori* countermeasures
  - Cryptographic authentication technologies
    - Based on ring signatures [LSHS07], [GGT06]
      - Messages are endorsed with ring signatures
      - Privacy provided by the anonymity of ring signatures
      - Vehicles cannot be traced (Privacy enhanced)
      - Vehicles producing fraudulent messages cannot be punished (Space left for attackers)

Countermeasures for securing VANETs (VIII)

- *A priori* countermeasures
  - Threshold-based [GGS04], [ODS07], [PP05], [RAH06], [DDSV08] with assumptions that
    - The more people endorse a message, the more trustworthy it is
    - There is a majority of honest vehicles
    - A message is trusted if it was endorsed by at least t vehicles
      - No privacy: Anonymity would allow one vehicle to behave like t vehicles
  - [DDSV08] provides anonymity, but it cannot be revoked
      - Secret sharing techniques
      - Threshold signatures

The [DDSV08] system (I)

- The car manufacturer generates
  - A public key **PK**
  - *n* fragments of his/her private key (using a threshold *t*)
    - $\mathbf{SK_1,\ldots,SK_n}$
- Each car-embedded communication device holds
  - Public key **PK**
  - Identifier **i**
  - Fragment of private key $\mathbf{SK_i}$

The [DDSV08] system (II)

- An announcement message is considered valid if
  - It carries a valid digital signature verifiable using **PK**
- Guarantees
  - External attackers cannot participate
    - They hold no information on the private key
  - At least t vehicles endorse the message

The [DDSV08] system (III)

- Message verification cost
  - New system:
    - **One** signature verification
  - System by [RAH06]:
    - *t* signature verifications
    - *t* certificate verifications
- Message length
  - New system: *O(1)*
  - System by [RAH06]: *O(t)*

The [DDSV08] system (IV)

- Message generation
  - Vehicle **i** sends (M, sig$_{\mathbf{i}}$(M))
- Message endorsement
  - Vehicle **j** receives (M, sig$_{\mathbf{i}}$(M))
  - Vehicle **j** checks information M
  - Vehicle **j** sends (M, sig$_{\mathbf{j}}$(M))
- Messages with limited range (no relaying)

The [DDSV08] system (V)

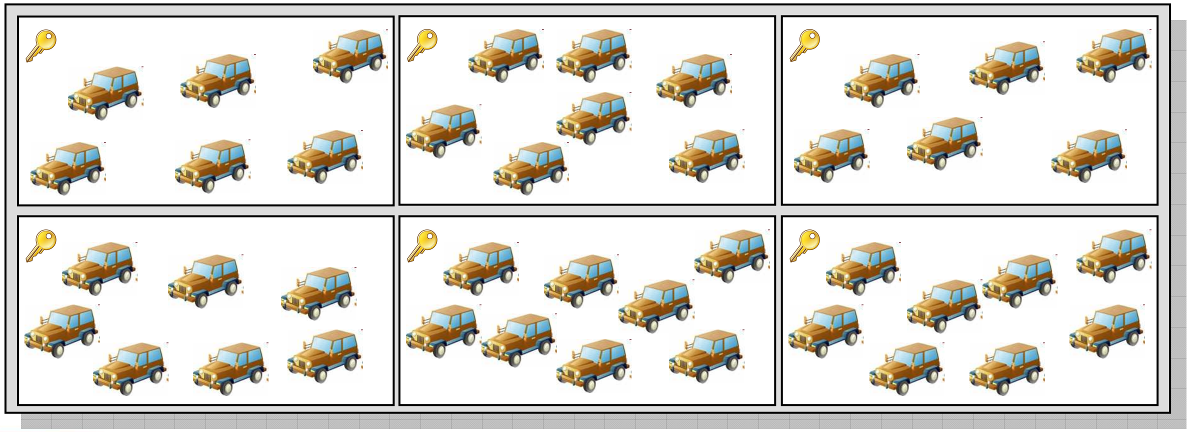
- Signature composition for a message
  - The generating vehicle stores
    - M, $\mathrm{sig}_i(\mathrm{M})$, $\mathrm{sig}_j(\mathrm{M})$, …
  - As soon as it collects *t* partial signatures
    - It generates and sends (M,sig(M))
    - The signed message is broadcast over a long range (with relaying if needed)

The [DDSV08] system (VI)

- Privacy
  - A completely signed message (M,sig(M))
    - Is verifiable using **PK**
    - Does not disclose information on the vehicles which took part in its generation
    - Offers privacy and unlinkability
  - A partially signed message (M,sig$_{\mathbf{i}}$(M))
    - Identifies node **i** (needed to compose signature)
    - Partial signatures are linkable
  - Partial signature privacy needed

The [DDSV08] system (VII)

- Group-based private protocol
  - The *n* vehicles are divided into *r* groups
  - Carmaker generates *r* private key fragments
  - Vehicles in the same group get the same fragment
    - The partial signature identifies the group
  - Composition requires partial signature by *t* vehicles from different groups



The [DDSV08] system (VIII)

- Group-based protocol (choice of the number *r* of groups)
  - *n/r* must be large enough for within-group privacy to exist
  - *r* must be large enough for *t* vehicles from different groups to be easy to find
  - Sparse traffic poses a problem

Discussion on existing countermeasures (I)

- *A posteriori* countermeasures alone are not sufficient
    - Taking strict punitive action can exclude some rational attacks (+)
    - Taking strict punitive action cannot prevent damages (-)
    - Taking strict punitive action cannot prevent irrational attacks (-)

Discussion on existing countermeasures (II)

- Existing solutions with *a posteriori* countermeasures use too strong assumptions:
  - There is a majority of honest vehicles in any case
    - What if a place is controlled by the organized crime?
  - There is a universally suitable threshold
    - How to find it?
    - Does the threshold depend on vehicle density?
    - Does the threshold depend on message importance?
    - Does the threshold depend on message urgency?
    - …

Discussion on existing countermeasures (III)

- Privacy is problematic with existing solutions
  - Some schemes do not provide privacy
    - Driving pattern can be extracted
  - The Sybil attack is possible in most anonymous schemes (except [DDSV08])
  - For [DDSV08], if a false message is generated in spite of a priori protection, no anonymity revocation is possible

Towards a combination of *a priori* and *a posteriori* countermeasures

- Security goal of our new design
  - Flexible threshold authentication
    - A vehicle can verify whether a received message has been endorsed by at least *t* vehicles
    - The threshold *t* can dynamically change according to the VANET context
  - Privacy preservation
    - An attacker cannot trace vehicles generating messages
  - Identity revocability
    - Trusted parties can trace vehicles generating fraudulent messages

Message-linkable group signatures (I)

- We presented in [DW09], [WDG09] a new primitive referred to as message-linkable group signatures (MLGS)
- There is a trusted group manager (GM)
- Vehicles can register to and obtain certificates from GM
- Group signatures of **different messages** from different signers are **indistinguishable**
- Group signatures of **the same message** from different signers are **distinguishable**
- Easy to tell whether two group signatures of the same message come from the same signer
- Only GM can trace the authors of group signatures

Message-linkable group signatures (II)

- Messages are endorsed with MLGSs
  - Tampered messages can be identified
- Message *m* is trusted if endorsed by t_m vehicles (*a priori* countermeasures)
- Privacy is provided by the anonymity of MLGSs
- GM can trace the identities of vehicles
- Vehicles producing fraudulent messages can be punished (*a posteriori* countermeasures)
- Fast signature verification techniques are provided to improve efficiency

Main references (I)

- [RPH06] M. Raya, P. Papadimitratos and J.-P. Hubaux. Securing vehicular communications. IEEE Wireless Communications Magazine, vol. 13, no. 5, pp. 8-15, 2006.
- [RH07] M. Raya and J.-P. Hubaux. Securing vehicular ad hoc networks. Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, no. 1, pp. 39-68, 2007.
- [RPAJ07] M. Raya, P. Papadimitratos, I. Aad, D. Jungels and J.-P. Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557-1568, 2007.
- [AFWZ07] F. Armknecht, A. Festag, D. Westhoff and K. Zeng. Cross-layer privacy enhancement and non-repudiation in vehicular communication. In 4th Workshop on Mobile Ad-Hoc Networks (WMAN), Bern, Switzerland, March 2007.
- [GBW07] J. Guo, J.P. Baugh and S. Wang. A group signature based secure and privacy-preserving vehicular communication framework. In Mobile Networking for Vehicular Environments, pp. 103-108, 2007.

Main references (II)

- [LSHS07] X. Lin, X. Sun, P.-H. Ho and 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.
- [GGT06] C. Gamage, B. Gras and A.S. Tanenbaum. An identity-based ring signature scheme with enhanced privacy. In Proceedings of the IEEE SecureComm Conference, pp. 1-5, 2006.
- [GGS04] P. Golle, D. Greene and J. Staddon. Detecting and correcting malicious data in VANETs. In Proceedings of the 1st ACM international workshop on Vehicular Ad Hoc Networks, pp. 29-37, 2004.
- [PP05] B. Parno and A. Perrig. Challenges in securing vehicular networks. In Proceedings of the ACM Workshop on Hot Topics in Networks, 2005.
- [ODS07] B. Ostermaier, F. Dötzer and M. Strassberger. 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.

Main references (III)

- [RAH06] M. Raya, A. Aziz and J.-P. Hubaux. Efficient secure aggregation in VANETs. In Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks -VANET 06, pp. 67-75, 2006.

- [DDSV08] V. Daza, J. Domingo-Ferrer, F. Sebe and A. Viejo. Trustworthy privacy preserving car-generated announcements in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 58(4):1876-1886, 2009.

- [DW09] J. Domingo-Ferrer and Q. Wu. Safety and privacy in vehicular communications. In Privacy in Location-Based Applications (eds. C. Bettini, S. Jajodia, P. Samarati and S. Wang), Springer, Chapter 3 (2009, to appear).

- [WDG09] Q. Wu, J. Domingo-Ferrer and . Gonzlez-Nicols. Balanced trustworthiness, safety and privacy in vehicle-to-vehicle Communications. IEEE Transactions on Vehicular Technology (accepted, September 2009).