СЕКЦІЯ: ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ЦИФРОВОЇ ОСВІТИ У ВИЩІЙ ТА СЕРЕДНІЙ ШКОЛІ УКРАЇНИ ТА КРАЇН ЄВРОСОЮЗУ

METHODS OF CRYPTOGRAPHY IN CAR2X SYSTEM

Uliana Iatsykovska
Department of Computer Science and Automatics,
University of Bielsko-Biala,
POLAND, Bielsko-Biala, 2 Willowa St
uiatsykovska@ath.bielsko.pl

Introduction. Cryptography has one of the main places in securing systems of Car2X. In the last of the fifteen years, was increased the impact of attacks on the car industry. Security and protection against malicious attacks, is the main problem to automotive manufacturers [1].

In the middle of the 1990 years was started the development of Cryptography in a car. Standardization of automotive security began in Germany. There are two large projects of telematics infrastructure such as Toll Collect and the Digital Tachograph uses smart cards extensively and methods of cryptography. This system was paid a lot of attention of the security challenges [2].

Nowadays, problems of security and cryptography for automotive are being studied on special conferences likes VDI Automotive Security or ESCAR. At general security conferences the problems of automotive security even becomes a main topic for discussion. For example, problems security in sphere of automotive was presented in the paper [3] or at CHES 2010 by Hovav Shacham [4].

Standardization for Car2X. The topic secure Car2X communication has a large number of publicly founded projects. They are the projects simTD, SEVECOM, and EVITA for Europe.

The large test field for Car2X functionalities is simTD. The application layer and Car2X Communication are definitely the subjects of this test, but security here has only of minor importance.

As for SEVECOM, it has been in focus the threat, vulnerability and risk analysis but followed by the general security architecture. For Car2X communication in this project define specific security mechanisms.

EVITA is focused on the secure hardware and software components, on the design of a secure automotive on-board network, and protocols for communication inside the car have been developed. That's three different types of security controllers. Asymmetric and symmetric cryptography performs light, medium and full hardware security modules corresponding to sensor, Electronic Control Units in Car2X communication.

Besides these projects there are at least three further European interest groups that was dedicated to Car2X security:

– Car2Car Communication Consortium (C2C CC) and research institutes, especially WG Security;

– Intelligent Transport Systems, Working Group 5 Security of European Telecommunications Standards Institute, Technical Committee;

– eSafety Security Working Group;

– The relevant standard for Car2X security in the USA is the Trial-Use Standard IEEE 1609.2 [5].

Car2X communication

Many systems use proprietary security mechanisms. Automotive industry has open problems of security toward to standards. The weaknesses of the systems had relatively little impact in this sphere. But Car2X communication is a new quality. And any information from the outside world that is transmitted through potentially insecure channels directly influences the behavior of a car and on the safety of the passengers as a whole. Car2Car and Car2Infrastructure communication connect cars to a completely is new communication system and Intelligent Transportation System (ITS) [6].

In Car2X communication the car is act as a receiver and as a sender. A car is act as a relay and to route messages to other cars. But other cars are not directly within reach of the author of the message. Therefore, weaknesses in the security architecture of Car2X communication can directly influence other cars and on their behavior and safety. Safety and privacy can be achieved by sound security system. That's why the concept of security Car2X communication is an essential part in Car2X communication. Sound security architecture plays an important role in the successful Car2X communication, in technologically and politically through acceptance by the users.

There are the following communicating parties in a Car2X system: car (vehicle), roadside station (RSS) and network infrastructure, that are presents on figure 1.

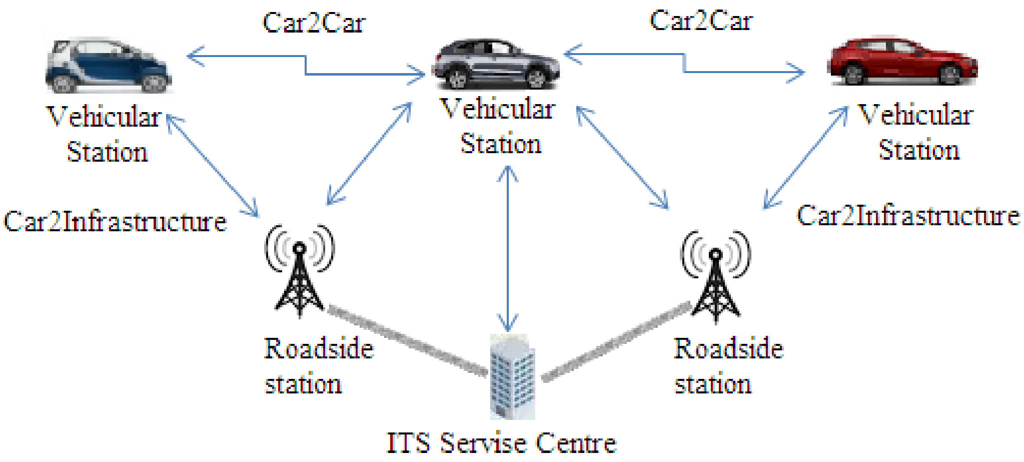

Figure 1: Communicating in a Car2X system

Example of communication in Car2X system [7]:

- Car2Car – short-time communication between car and car;
- Car2Infrastructure -short-time communication between car and roadside station;
- the communication between car and network infrastructure;

- the communication between network infrastructure and roadside station.

Methods of cryptography

Security objectives are to authorized users should be able to participate in the system and privacy aspects have to anonymity and non-traceability. For Car2X communication the main cryptographic problem is to protect many, relatively short messages, which have to provide integrity of data. The data has to be encrypted in many cases too. Latencies are very critical when the communication happens in unicast mode or broadcast.

As for standard security objectives such as integrity and freshness of data, non-repudiation, optional confidentiality can be achieved by cryptographic methods.

Symmetric methods can use for signature proposal in Car2X. And security system can be established with from a secure master key and key encryption/transport. As for security objectives, they can be achieved with symmetric methods, except non-repudiation. But, method of symmetric cryptography is not optimal with broadcast messages [8].

Asymmetric methods are purely solution in the form of digital signatures has been discussed. When the all parties of the Car2X system obtain digital certificates and sign all their messages by private key. And the recipient verifies the integrity of data by signature verification. For medium to high security requirements can use cryptosystem RSA. Signature in RSA system is competitive, but cars have to verify and very often they have to sign messages by themselves. Signature generation by RSA for 2048 bit length is longer and prohibitive expensive [9].

Instead of RSA cryptosystem can be use Elliptic Curve Cryptography (ECC). Cryptography methods by Elliptic Curve have moderate key and signature length [10]. Methods of Post Quantum Cryptography are specially designed for long-time security. Very good security properties have a Merkle Hash Tree method. There are extreme length of public key and signature in this method and seems not good for this use.

Hybrid methods combine as symmetric and asymmetric methods. In this case the temporal symmetric key is encrypted by a public key encryption algorithm. Integrity and encryption of mass data in Car2X system is done by symmetric methods. That's solution perform the combination of symmetric and asymmetric methods in a more systematic and was describes in [11]. Modern hybrid encryption schemes consist of a Data Encapsulation Mechanism and of a Key Encapsulation Mechanism. In ECIES method ElGamal encryption is used as Key Encapsulation Mechanism [12].

Summary. With a reliable security system will be successful Car2X Communication. But in resolving the privacy issue, Car2X Security will be accepted only for the public. The performance requirements for security in Car2X system are rather high. The Wireless Access in Vehicular Networks Security standard consists of asymmetric digital signature scheme and a symmetric authenticated encryption scheme, a hybrid encryption scheme and is the best nowadays.

References:

1. Daniel Ohst. Security aspects of road tolling – requirements from a toll service provider. In Proceedings of escar 2007, Embedded Security in Cars, Munich, November 6, 7, 2007, 2007.

2. Furgl I., Lemke K. A review of the digital tachograph system. In K. Lemke, C. Paar, and M. Wolf, editors, Embedded Security in Cars, pages 69–94. Springer, 2006.

3. Koscher K., Czeskis A., Roesner F., Patel S., Kohno T., Checkoway S., McCoy D., Kantor B., Anderson D., Shacham H., Savage S. Experimental security analysis of a modern automobile. In D. Evans and G. Vigna, editors, Proceedings of IEEE Security and Privacy, pages 447–462. IEEE Computer Society, 2010. see http://www.autosec.org/pubs/cars-oakland2010.pdf.

4. Hovav Shacham. Cars and voting machines: Embedded systems in the field, 2010. Invited talk at CHES 2010, Santa Barbara.

5. IEEE P1609.2. Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages, 2006.

6. ETSI TS 102 637-1. Intelligent Transport Systems (ITS); Vehicular Communication; Basic Set of Applications; Part 1: Functional Requirements, 2010.

7. ETSI TS 102 637-3. Intelligent Transport Systems (ITS); Vehicular Communication; Basic Set of Applications; Part 3: Specification of Decentralized Environmental Notification Basic Service, 2010.

8. Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani. On the power of power analysis in the real world: A complete break of the KeeLoq code hopping scheme. In D. Wagner, editor, Proceedings of CRYPTO 2008, volume 5157 of Lecture Notes in Computer Science, pages 203–220. Springer-Verlag, 2008.

9. Holger Bock, Michael Braun, Markus Dichtl, Erwin Hess, Johann Heyszl, Walter Kargl, Helmut Koroschetz, Bernd Meyer, and Hermann Seuschek. A milestone towards RFID products offering asymmetric authentication based on elliptic curve cryptography. In Proceedings of RFIDSec 2008, the 4th Workshop on RFID Security, Budapest, Hungary, July 2008, 2008.

10. Manfred Lochter and Johannes Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. Internet Request for Comment RFC 5639, Internet Engineering Task Force, March 2010. see http://www.rfc-archive.org/getrfc.php?rfc=5639.

11. ISO/IEC 18033-2-2006. Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers. ISO/IEC, 2006.

12. ANSI X9.63-2001. Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. American Bankers Association, 2001.

FORMATION OF INFORMATION AND COMMUNICATION COMPETENCY OF FUTURE SPECIALISTS OF THE AUTOMOBILE TRANSPORT FIELD

Salnikov Bohdan Volodymyrovych
student of speciality «Road traffic management and handling»

Symkovych Rostyslav Mykolaiovych
student of speciality «Organisation of transportations and transport management»,
Motor transport college of the State Institution of Higher Education
«Kryvyi Rih National University»
amoak@i.ua

Specificity of scientific and technological progress in modern society requires from the automobile industry specialist the flexibility of thinking, the ability to improve and to maintain their cognitive activity, in order to diagnose their own level of professional development. In the conditions of rapid development of information and communication technologies, it is important to raise the level of our own information culture. This theme is of current interest.

V. Bespalko, Y. Vargamenko, A. Yershov, M. Zhaldak, Y. Mashbits, I. Robert, S. Nikolaenko and other scientists made a significant contribution to the theory and practical use of information technologies. The research of scientists proves that "one of the important factors in the intensification of the educational process is the use of