MODERNISATION OF TECHNOLOGY AND EDUCATIONS
METHODS ORIENTATED TO AREA OF CRYPTOGRAPHY FOR
SAFETY CRITICAL APPLICATIONS

Mária Franeková
maria.franekova@fel.uniza.sk

University of Žilina, Faculty of Electrical Engineering, Univerzitná 1, 010 26 Žilina
SLOVAK REPUBLIC

Key words: Safety critical applications, safety-related communications system, cryptography, European Train Control System, Euroradio protocol, Key Management System, symmetric cryptography, mechanisms of enciphering, digital signature schemes, equivalent security, computationally safety, educations, e-learning

Abstract: Inseparable part of education orientated to safety is area of safety communications, which contents cryptography part too. Requisites of subjects development at technical universities in specialisation of Automation is result of request from praxes where in last decade was notified development of applications which used safety-related communication system (e.g. area of industrial applications, safety-related control and communications systems in railway or road applications). Pedagogical staff of Department of Control and Information Systems at University of Žilina has sufficient theoretical and practical knowing which can used within realisation of project KEGA orientated to modernisation of education methodology with using modern HW and SW cryptography tools. It is new perspective discipline based on using cryptography in applications with increasing safety integrity level (SIL) which needs transfer of knowledge of the newest e-learning technology of educations to educations process at home university and partner’s Todor Kableshov University too.

Cryptography techniques are became in the last several decade the generally assurance mechanisms within COTS (Commercial Off The Shelf) technologies but in the safety critical application they are recommended to use in the last years only. Selection of cryptography technique, modes of operation and methods related with key management system must be realized in consequence with the norm valid for safety related messages transmission.

Several part of cryptography systems are in phase of developing and concerning to very dynamic developing discipline from the area of cryptanalytic attacks several recommended cryptography mechanisms are inapplicable in EURORADIO protocol. This is why it is necessary considering the computational safety of cryptography mechanisms, consider their selection and design KMS (Key Management System) for these algorithms. Recently KMS for ETCS system in L2 in particular European countries in phase of development and decisions, whereby the selection of off-line or on-line KMS are solved and which principles of KMS will be supported (symmetric or asymmetric cryptography systems).
KMS solves without generation of keys additional important procedures of key manipulations (e.g. store, distribution, changing) whereby these procedures must be solved on the safety manner and control within the life time of cryptography system. The next question which will be solved in the future is question about CA (certification authority) for KMS within European countries for ETCS system. In considering of interoperability of railway transport in Europe these procedures and agreements must be the same and all questions must be solved uniform in EU countries with connection to states of near continents.

1. Introduction

Cryptographic techniques are primarily used in security critical applications. However, there may also be useful applications of cryptographic techniques in safety critical systems mainly in very important sub-part of this system - communication parts.

Main reasons of cryptography using in area of open networks are based on reality that networks include ground useful attributes in the form of HW, SW, data and transmission media where is difficult to control access of illegitimated object/subjects, whereby they introduce large risk of treats within information safety.

There are basically two types of cryptographic systems: symmetric and asymmetric cryptographic systems [1], [2]. A symmetric cryptographic system applies the same key for encryption and decryption. An asymmetric cryptographic system applies different keys for encryption and decryption. For a cryptographic system to work as intended something must be kept secret for everybody except the sender and the intended receiver. In most systems the key is the secret part, whereas the encryption/decryption algorithm is public. Many symmetric or asymmetric algorithms were developed in parallel with methods of key management system. Only several of them are recommended to use in safety critical applications, where a failure can cause damage on persons, property or the environment. Today it is well known the cryptography standards for commercial sphere (e.g. financial sector, company information systems ...), e.g. [3] but for applications of cryptography with increasing safety integrity level (SIL) the methodology for safety evaluations absent.

Cryptographic techniques are recommended to apply within safety-related application (e.g. safety-related control system in railway transport or dangerous industrial process control) if malicious attacks within the open transmission network cannot be ruled out. This is usually the case when safety-related communication uses a public network, a radio transmission system, wireless technology (Wi-Fi, ZigBee,…) and a transmission system with connections to public networks. Cryptographic techniques can eliminate masqueraded of message and support confidence of transmission, authentication of source messages and message integrity which can be corrupted during transmission. The most well-known code is the message authentication code MAC that is standardised in ISO/IEC 9797-1 and ISO/IEC 9797-2, which is recommended to use within safety critical railway application euroradio system developed within ETCS [4].

The safety related machine builder usually buys a commercial communication system (COTS), which includes several features to ensure reliability and safety. The machine builder needs to verify that the system is adequate for the intended purpose. COTS with features that do not fulfil the safety requirements of the current system shall not be used. A solution could be to compensate reliability short comings by adding safety features to the application. In wireless communication we cannot ensure reliability since, e.g. with increasing distance between transmitter and receiver, errors become more probable and finally the connection is lost. At system level it is possible to e.g. use two transmitters and different frequencies. This
helps a little but, again, if distance increases the connection is lost. The duplication of devices helps to minimise the effects of component failure, but does not solve the reliability problem.

2. **Enforced access by using cryptography in safety-related applications**

Access by applying cryptography within communications between safety-related (SR) equipment in safety-related communication systems we can divide to two solutions [5] (see Fig. 1):

- Cryptography tool is part of SR concrete equipment - (layer of access protection – in Fig. 1 illustrated by blue colour).
- Cryptography tool is part of safety measures of several SR equipment, which communicate within internal network and they are implemented into separated layer of access protection (in Fig. 1 illustrated by yellow colour). This access is more enforced and recommends using of firewall, which must be component of safety analyses of SR application.

![Fig. 1 Enforced access within implementation of cryptography in SR communications system](image)

3. **Specifications of cryptography techniques for safety critical applications**

By comparison with COTS (Commercial Off The Shelf) technology for using cryptography in SR applications are necessary to keep the following specifications:

- **Limited computationally performance of equipment** - in any applications (e.g. 8-bit architecture) is difficult applying of principles of modern – mainly asymmetric cryptography, which is based on difficult mathematical operations from number theory and modular arithmetic.
• **Needed reaction within data transmission in real time** – performance of cryptography operations must be realised in real time, to be required time of response kept.

• **Effectiveness management of cryptography keys** – in addition to implementation of cryptography algorithms it is necessary to solve in real time key management (key is biggest weakness of cryptography protocols), cryptography solutions are incomplete without key management.

The most recommended cryptography techniques in Safety-related communication system are combined encryption schemes with digital signature. All digital signature schemes are based on safety of one-way hash functions. In consideration of limited space we mentioned at least table survey of computationally safety algorithms which are recommended to use in SR applications. Security of cryptography algorithm we can describe via term equivalent security, which presents how is decreased the length of key (in bits) by the make provision for effect of nowadays known cryptanalytics attacks to algorithms.

In the Table 1 are compared the lengths of keys for keeping the equivalent safety for symmetric cryptography systems (2DES, 3-DES, AES) and asymmetric cryptography systems (RSA and ECC). Nowadays the algorithms in orange fields are considered as computationally safety.

### Tab. 1 Comparison of key lengths of cryptography algorithms

<table>
<thead>
<tr>
<th>Equivalent safety of cryptography algorithms [bit]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length of key of symmetric algorithms</td>
</tr>
<tr>
<td>80 (2DES)</td>
</tr>
<tr>
<td>112 (3DES)</td>
</tr>
<tr>
<td>128 (AES-128)</td>
</tr>
<tr>
<td>192 (AES-192)</td>
</tr>
<tr>
<td>256 (AES-256)</td>
</tr>
</tbody>
</table>

4. **Transfer of keeping knowledge to education process**

Results of project KEGA 024ŽU- 4/2012: “Modernization of technology and education methods orientated to area of cryptography for safety critical applications” during years 2012 to 2014 we can divide to the following areas:

**Area of railway and road transport**

- Monitored fields within scientific areas:
  - ETCS (European Train Control System) – development of unified system for control of railway transport.
  - EURORADIO protocol – using of mobile network GSM – R. Euroradio is developed in SIL4.

LDWS system – detection of deflection from driving line via modern methods of image processing with connection to VANET.

Area of control and communications system used in industry applications

- Monitored fields within scientific areas:
  - safety Ethernet,
  - wireless technology – perspective transmission media for safety-related applications.

Within presented themes it was necessary to solve the following problems:

- authentication of entities within transmission of safety-related messages in ETCS system with using cryptography mechanisms, development of methods for on-line key management system, development of methods for safety evaluation of cryptography transmission,
- development of applications with orientation to safety and their integration, development of effectiveness methods of transmission of authentication messages in VANET networks with using cryptography schemes of digital signature on the base of elliptic curves (ECDSA),
- risk analysis, modelling of safety features of control and communication system with using open transmission systems,
- safety-related applications with wireless communications,
- safety analyses of communications with using cryptography tools for applications with increasing SIL.

Invited or required lectures in foreign universities:

- Cryptography and its applying within safety – critical applications, (prof. Ing. Mária Franeková, PhD.), Silesian University of Technology, Faculty of Transport, Katowice, Poland, 2012
- Safety evaluation of the signalling systems, (prof. Ing. Karol Rástočný, PhD.), Silesian University of Technology, Faculty of Transport, Katowice, Poland, 2012
- Safety evaluation of data transmission within safety – related control systems. (prof. Ing. Mária Franeková, PhD.), Todor Kableshkov University, Sofia, Bulgaria, 2012 (Erasmus program)

Publications of working group related with given problems:
Selection of relevant publications we can see in references [6], [7], [8], [9], [10], [11].

Themes of PhD works related with given problems:

References


Acknowledgements
This paper was supported by the scientific grant agency KEGA No. KEGA 024ŽU-4/2012: Modernization of technology and education methods orientated to area of cryptography for safety critical applications
MOДЕРНИЗАЦИЯ НА ТЕХНОЛОГИИТЕ И МЕТОДИТЕ ЗА ОБУЧЕНИЕ В ОБЛАСТТА НА КРИПТОГРАФИЯТА ЗА ПРИЛОЖЕНИЯ ПО КРИТИЧНА БЕЗОПАСНОСТ

Mária Franeková
maria.franekova@fel.uniza.sk

Университет Жилина, Електротехнически факултет, Univerzitná 1, 010 26 Žilina SLOVAK REPUBLIC

Ключови думи: приложения за критична безопасност, комуникационна система за безопасност, криптография, Европейска система за управление на влаковете, Euroradio протокол, симетрична криптография, механизми за шифриране, схеми за електронен подпис, еквивалентна сигурност, обучение, електронно обучение.

Резюме: Неразделна част от образованието, ориентирано към безопасност, е областта на комуникациите за безопасност, част от чието съдържание е и криптографията. Развитието на учебната дисциплина в техническите университети, в специалността по автоматика, е резултат от потребностите на практиката, където през последното десетилетие е сертифицирано разработването на приложения, които се използват във връзка с безопасността на системата за комуникация (например в областта на промишлените приложения, системи за управление на безопасността и комуникационните системи, свързани с приложения в железнодоръчния или автомобилния транспорт). Преподавателският състав в Катедрата по управляващи и информационни системи в Университета в Жилина има достатъчни теоретични и практически познания което може да се използва в рамките на реализацията на проекта KEQA с цел модернизация на методологията за обучение с помощта на съвременни хардуерни и софтуерни криптографски инструменти. Това е нова перспективна дисциплина, базирана върху използването на криптографията в приложения за повишаване на равнището на цялостната безопасност (SIL), която се нуждае от трансфер на знания за най-новите технологии за електронно обучение към образователния процес в нашия университет, а също така и в партньорския университет ВТУ «Тодор Каблешков» университет.

През последните няколко десетилетия криптографските техники се превърнаха в общи механизми за сигурност в рамките на технологите COTS (Commercial Off The Shelf), но приложението им при критична безопасност се преръщва една от няколко години. Изборът на техника, криптография, режими на работа и методи, свързани с ключовите системи за управление трябва да бъде реализиран в съответствие с нормите, които са валидниза предаването на съобщения, свързани с безопасността.