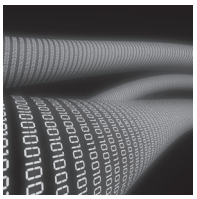

Archives of
Transport System
Telematics

Volume 2

Issue 1

February 2009

Key Management System in ETCS

M. FRANEKOVÁ[a], P. CHRTIANSKY[b]

[a] Faculty of Electrical Engineering, University of Žilina, Univerzitná 1, 01026 Žilina, Slovakia,

[b] Tempest, a. s., Plynárenská 7/B, 821 09 Bratislava, Slovakia,

EMAIL: maria.franekova@fel.uniza.sk

ABSTRACT

Paper deals with problems of KMS (Key Management System), which is developed in mobile communications GSM-R (Global System Mobile for Railway) recommended within the European Train Control System (ETCS), through the Euroradio system. The main part is oriented to safety procedures description of off-line KMS system between communication entities of ETCS system. In the experimental part the results of computational safety of modified DES algorithm are summarised using special brute force attack to key – birthday paradox.

KEYWORDS: mobile communications, open transmission system, key management system, radio block centre, key management centre, on board unit, brute force attack, birthday paradox

1. Introduction

Social and economic aspect and economical significance of railway transport are large within integrating and expanding European Union. Special emphasis is put on requirements of interoperability, safety and increasing the quality of provided services, what is connected with increasing the speed and capacity of transport network. A project of ERTMS (European Rail Traffic Management System) and its components: ETCS (European Train Control System) and GSM -R (Global System for Mobile Communication for Railway) responds to these requirements.

Digital cellular radiotelephone system GSM (Global System for Mobile Communications) is the industry standard used by the greatest European telecommunication operators and vendors of equipments. The GSM-R network as the technological basis for open communication system within railway transport was chosen and specified within projects EIRENE and MORANE of UIC (International Union of Railways). The EIRENE project eventuated in specifications of the system and functional requirements, which provide basic framework of interoperability within mobile communications on the railway. The results are documents [1], [2], which define a set of requirements of radio communication system for railways. They issued from ETSI GSM standard, but they expand this standard with special requirements towards interoperability, safety and performance of systems according to the needs of the railway transport.

ERTMS/ETCS system consists of a stationary part installed in adequate places along a railroad, and of a mobile part installed on track vehicles. ERTMS system is divided up into three different equipment and functional levels (application levels L1, L2 a L3). In areas equipped with application levels L2 and L3, the messages for train control are executed by RBC (Radio Block Centre) based on actual information from the interlocking equipment. The structure of stationary and mobile parts of ETCS system and characteristics of application levels of ERTMS/ETCS are described in detail e. g. in [3]. As it is illustrated in fig. 1, the communication stream between different Euroradio units can run through several networks such as mobile networks (GSM-R) and PLMN (Public Land Management System),

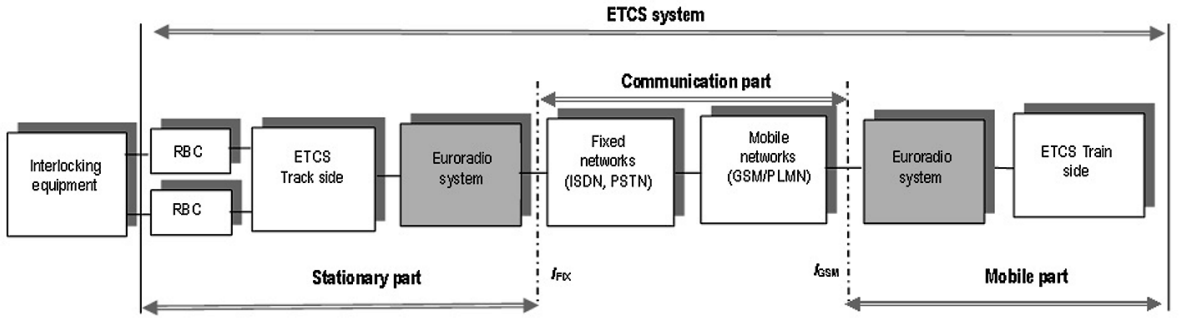

Fig.1. General architecture of Euroradio/ETCS system
Source: [6]

fixed networks ISDN (Integrated Service Digital Network) or PSTN (Public Switched Telephone Network). Every network has its own internal structure and communication protocol. The Euroradio system establishes connection with network interfaces I_{GSM} on the side of mobile networks and IF_{IX} on the side of fixed networks.

For communication in GSM-R network GSM-900 standard is used, which includes standard and extended GSM-900 band. For transmission from a mobile station to base stations subsystem (uplink) frequencies 876 – 915 MHz and channels 955 – 1023 are recommended, and for transmission of opposite direction (downlink) frequencies 921-960 MHz and channels 0 – 124 are used. In addition, GSM-R provides special services for use in railway transport.

GSM-R mobile system, as a communication system of Euroradio, is ordered according to norms for railway applications between open transmission systems with class 6 to 7, with the assumption of high level of threat within messages transmission as a result of EMI (Electromagnetic Interference) or influence of other passive or active attacks on a message. The method of telegram construction

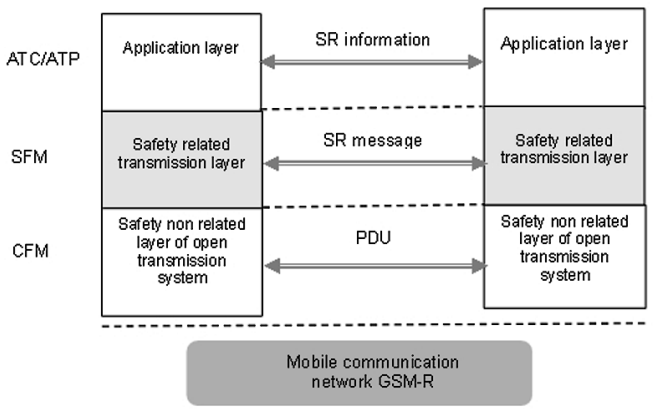

Fig.2. Principle of communication between safety related subsystems with using GSM-R
Source: [7]

in Euroradio protocol corresponds with A1 type message model, marked in [4] as using a cryptography code with secret key. I. e. cryptography which has been up to now a domain of commercial field (banking, e-commerce, ...), begins to use in safety-related railway communication systems GSM-R. It is important to underline, considering the dynamic evolution of crypto analysis (attack on key or algorithm), that it is necessary to revalidate more frequently the safety of recommended standards and to modify it flexibly toward using a safety mode of algorithm or to supply new cryptography standards. In a symmetric cryptography system which is recommended in Euroradio communication protocol, the most vulnerable part of the system is the key management system (from key generation to key distribution and its storage). The question of key's length is especially sensitive concerning a brute force attack and nowadays well know modification of brute force attack e. g. birthday attack. Methods of KMS are still developed within ETCS project and direct from off line KMS system to on-line system [5].

2. Safety-related layers within Euroradio systems

Communication between stationary and mobile parts is based generally on principles of safety-related communication. Safety related layers are realised with the use of SFM (Safety Functional Module). The principle of safety-related communication between safety-related subjects using an open transmission GSM-R system is illustrated in fig. 2.

The SFM module is implemented in the ETCS system by two safety related layers:

- Safety layer of Euroradio [6],
- SAI (*Safety Application Interface*) [7].

Layersare implemented over RM OSI transport layer, between safety-related layers and the transport layer is implemented in the adaptation layer.

The Euroradio safety layer provides defence against the following threats: corruption of messages, insertion and masquerade of messages. Safety procedures of Euroradio SL include authentication and data integrity of message during transmission. Both procedures are carried out using MAC (Message Authentication Code) [6]. Safety-related layer SAI provides defences against the following threats: delay, resequence, deletion and repetition of messages. The layer uses the following defences: sequence number and time stamp [7].

The paper focuses on the key management system for safety-related layer Euroradio SL only.

3. Key management system

For assurance of interoperability within ETCS/ERTMS system class 1 [5] it is necessary to specify the requirements of KMS (Key Management System) too. In the first phase off-line KMS is recommended, where distribution, revocation or updating of any key requires staff intervention. KMS in ETCS system is created on the basis of symmetric cryptography.

General requirements for off-line KMS system can be summarised as following:

- KMS structure of must be simple.
- KMS must use the standard protocols/algorithms.
- KMS must be able to change keys a safety way.
- unauthorised person cannon read from storage keys.
- An attack on key materials must be detected.
- Unauthorised objects must not be able to modify keys computationally during transmission.

In ETCS system it is necessary, for KMS needs, to consider the following questions in KM (Key Manager):

- Key generation – generation of keys for ciphering/deciphering or for authorised persons and processes in a well defined organisation and secure environment. Each generated key shall be uniquely identified. The keys should be generated randomly.
- Key validation – checking all generated keys to guarantee that they are not weak or semi-weak keys.
- Store of keys – storage of keys (operation must be authenticated and confidential).
- Key distribution – transmission of keys to train or trackside entities shall be under the responsibility of the KMC domain. It shall be performed in a secure way and include all related key information.
- Key installation – installation of keys in trains or trackside entities (must be carried out in a secure way).
- Key derivation – derivation of session keys (on the master key – relation keys principle).
- Key deletion – deletion of keys (the procedure must be performed in a secure way).
- Key archiving - archiving of all keys and key related material by the KMC domain in an authenticated and confidential way.

All operation is necessary to regard during life time of cryptography system and to eliminate unauthorised access or modification of key related material.

Subset [6] defines the following hierarchy of keys:

- *Level 3* - transport key KTRANS: Protection of KMS communication between several KMC and ERTMS entities: RBC (Radio Block Centre) or train side unit OBU. Keys for connection protection between KMC are marked as K-KMC.
- *Level 2* – authentication keys KMAC: Authentication of ERTMS entities (OBU and trackside) during Euroradio safe connection establishment.
- *Level 1* – session keys KSMAC: Authentication of data transfer between ERTMS entities (OBU and trackside) during a complete safe communication session.

The following table (tab. 1) summarises different types of keys and their respective usage.

The basic concept of key management between two KM (Key Manager) domains may be seen in fig. 3. The key manager domain is defined by one KMC and all the on-board units and trackside entities using that KMC for any key purpose. The OBU KMAC may be installed in trackside entities in any number of KM domains, in which the onboard entity is authorised to run.

K-KMC keys are used to assure KMAC keys transaction between domains. K-KMC keys should be distributed between domains before activation of any transaction. KMC includes two parts of 192 bits. The first part of key, K-KMC1,

Table 1. The use of cryptography keys within ERTMS

Involved entities	The use of cryptography keys			Note
	Identification & Authentication	Message authentication	Ciphering	
RBC - OBU	KMAC	KSMAC	-	Relevant for interoperability
KMC - RBC/OBU	-	-	-	Domain specific
KMC - KMC	-	K-KMC1	K-KMC2	Relevant for interworking

Table 2. The results of SW realisation of birthday attack to modified cipher DES

Characteristic	Maximal number of experiments in one realisation			
	2^{12}	2^{13}	2^{14}	2^{15}
Number of realisations	1000	1000	1000	1000
Number of successful realisations	68	226	639	984
Number of unsuccessful realisations	932	774	361	16
Effective length of key k [bits]	28	28	28	28
Probability of successes P_S*	0,068	0,226	0,639	0,984
Predicted probability of successes P_S	0,061	0,221	0,632	0,982
Average number of realisations	3949,888	7228,148	10811,649	11353,897
Average time of realisation of attack [s]	0,077	0,147	0,234	0,282

is used for assurance of integrity and authentication of transaction using CBC-MAC algorithm. The second part of key, K-KMC2, is used for assurance of data confidentiality during transaction, consequently for ciphering of KMAC key.

For that purpose K-KMC2 is divided to three sub-keys K_1, K_2, K_3, each 64 bits (without parity bits) long. In the same way key KMAC is divided to three 64-bit blocks. Then every block is ciphered and deciphered using 3-DES algorithm (as it is illustrated in fig. 4).

4. Birthday attack

Many cryptanalysis works were published on expansibility and popularity of DES algorithm, which describe theoretical attacks on the algorithm possibly more efficient than brute-force attack. Theoretically, there are three known attacks that can break the full sixteen rounds of DES with less complexity than a brute-force search of the key space (that is, testing all possible keys in order to recover the plaintext used to produce a particular cipher text, in this case 2^{56} trials): differential cryptanalysis (DC), linear cryptanalysis (LC) and Davies' attack, from which the best is LC, which requires 2^{43} known plaintexts and has a time complexity of 2^{39-42}. [9]

Using 3-DES in CBC-MAC algorithm within Euroradio SL it is possible to predict modified brute-force attack on the authentication code i.e. birthday paradox. The birthday paradox is often presented in elementary probability courses to demonstrate that probability results are sometimes counteractive. The problem can be stated as follows: what is the minimum value of k such that the probability is greater than 0.5 that at least two persons in a group of k people have the same birthday? This problem can be described mathematically as:

$$p(365,k) \geq 0{,}5 \qquad (1)$$

This problem can be applied within the computation of authentication code duplicities. That is determination of computational complexity of one of basic requirements for authentication function C called collision resistant. To determine the probability, which describes the occurrence of duplicity within calculation of authentication code for

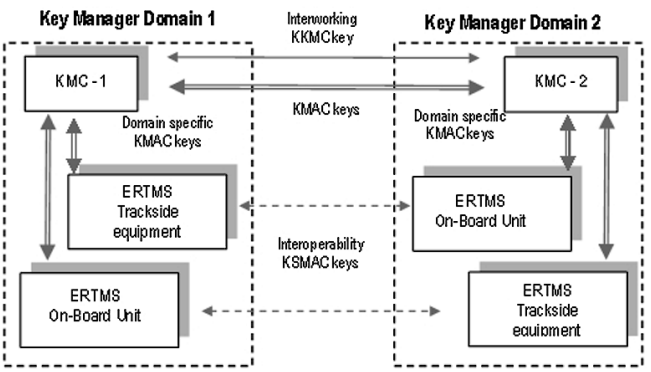

Fig. 3. KM context diagram
Source: [5]

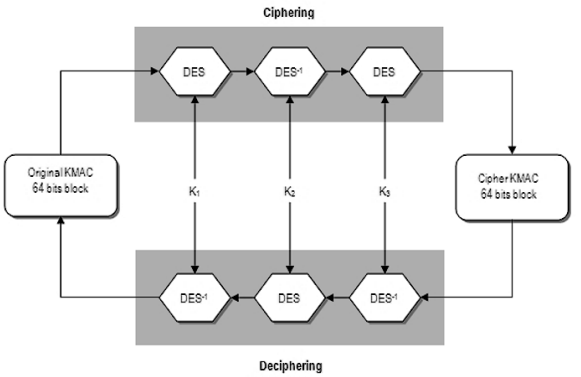

Fig.4. Ciphering of authentication key KMAC using K-KMC2 (K1, K2, K3) and 3-DES
Source:[7]

two different messages M_1 a M_2, i.e. $MAC_1=C_k(M_1)=MAC_2=C_k(M_2)$ we can use equation [8]:

$$P(n,k) = 1 - \frac{n!}{(n-k)!n^k} \quad (2)$$

Where n is the number of all messages, k is the number of messages, which we must generate for one collision occurrence. Equation (2) may be approximated as:

$$P(n,k) \approx 1 - e^{-(k.(k-1)/2n)} \quad (3)$$

The answer to question: what value of k is required, such that $P(n, k) \geq 0.5$, may be provided by (4). Then for k:

$$k \approx \sqrt{2\ln(2)n} \approx 1{,}18\sqrt{n} \approx \sqrt{n} \quad (4)$$

If the authentication code is m bits long, the number of all messages is $n = 2^m$. Using the approximation in equation (4) the number of calculated messages, which can be generated for the occurrence of one collision is:

$$k \approx \sqrt{n} = \sqrt{2^m} = 2^{m/2}. \quad (5)$$

Equation (5) achieved, that theoretical power of message authentication code with length of m bits long is bounded by the square root of code (or key) dimension.

The Possibility of calculation of one from n keys is described by relation (6). While $l.n \geq 2^k$ is selected, the probability of finding key P_S is high (e. g. $l = 2^{k/2}$, $n = 2^{k/2}$), where l is the number of randomly selected keys. Theoretical power of algorithm DES used in operation CBC-MAC is $O(2^{56/2})=O(2^{28})$ only.

$$P_S = 1 - \left(1 - l.2^{-k}\right)^n = 1 - \left(1 - \frac{1}{2^k/l}\right) \geq 1 - e^{-l.n/2^k} \quad (6)$$

5. Experimental part

Inthe experimental part a simple software application was developed, which allows verifying some of theoretical assumptions. A modified cipher DES with effective key's length of 56 bits was chosen as the optimal reference candidate. So a birthday attack needs for finding of the first key with high probability $2 * 2^{28}$ records (memory cell) and the same number of ciphering (if we consider within application the simulation of message obtaining with using of different keys). Software application was realised on PC laptop HP Compaq nx7300 with two-kernel processor Intel Centrino Duo with frequency 2 GHz and RAM 2 GB, frequency 997 MHz. The effective key length was reduced to 26 bits. Then computational complexity of a successful attack was on average $2^{14} = 16384$ records.

The results of experiment are presented in the tab. 2. Predicted probability of success was determined according to relation (6), $k = 28$, $l = n = k / 2$. Practical probability of success within experiment P_S^* is calculated with using empirical relation as ratio of number of experiment successful realisations to the number of all realisations.

6. Conclusion

In Euroradio system it is necessary to give remark to the key management system, which is a very sensitive part of global cryptography system, especially if symmetric cipher system is used. In this article we have shown that the use of 3-DES algorithm in authentication procedure of CBC-MAC and in KMAC encryption procedure is less secure than might be expected. Theoretical power of message authentication code m bits long is bounded by a square root of code, what is a result of modified brute force attack, called a birthday attack. In the experimental part a theoretical assumption of birthday paradox on modified DES algorithm was made. In the future a change of 3-DES algorithm to standard AES/Rijndael is recommended as an alternative solution, what corresponds to equivalent recommendations and development in the field of commerce

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0040/08 "Mathematic-graphical modelling of safety attributes of safety-critical control systems".

Bibliography

[1] UIC EIRENE SRS: System Requirements Specification, 2006, PSA167D006-15
[2] UIC EIRENE FRS: Functional Requirements Specification, 2006, PSA167D005-7
[3] ZÁHRADNÍK J. - RÁSTOČNÝ K.: Applications of interlocking systems, EDIS, ŽU Žilina, 2006, ISBN 80-8070-546-1
[4] EN 50159-2: Railway applications – Communication, signalling and processing systems. Part 2: Safety-related communication in open transmission systems, 1998
[5] Subset-038: Off-line Key Management FIS, 2005, v 2.1.9
[6] Subset-037: Euroradio FIS, 2005, v2.2.5, rev. G
[7] FIS between trackside sub-systems, Safe application service, version 8_0, 2002
[8] STALLINGS W.: Cryptography and Network Security, Prentice Hall, New Yersey, 2003
[9] BIHAM E.: How to Forge DES-Encrypted Messages in 2^{28} Steps, Technical Report, Department of Computer Science, Technion, Haifa, 1996, CS 884