Concept of Complex Cryptographic Protection for Telecommunication Networks

Karel Burda

Brno University of Technology, Brno, Czech Republic

Summary
The cryptographic protection is used to ensure the confidentiality and authenticity of information transmitted between the terminals of information and communication systems. Contemporary development indicates a new trend where the cryptographic protection is used not only between two terminals but also between the terminal and the access point to the network. In this paper, the principle of cryptographic protection in the access network is extended to the entire telecommunication network.

Keywords:
cryptographic protection, telecommunication network.

1. Introduction

An intensive exploitation of electronic systems is typical of contemporary society. Electronic systems ensure information transmissions (communication systems), enable an information management (information systems) or ensure the control of other systems (control systems). The functioning of a number of social processes (supply, production, business, etc.) is not possible without large electronic systems.

With the increasing significance of these systems for society functioning, efforts aimed at disabling electronic systems are getting more intensive. Therefore, a number of countries work on the protection of their electronic systems against attacks by terrorists or other countries. The significance of the protection of these systems is therefore growing.

The paper is concentrated on the improvement of the security of electronic systems through the cryptographic protection of telecommunication networks that are used by these systems.

2. State of the art

Cryptographic protection is a type of protection that is based on the impossibility or on the difficulty of solving some mathematical problems. In this connection, it is necessary to stress that practically used cryptographic mechanisms do not provide absolute security. There are a number of attacks on particular types of cryptographic mechanisms and therefore their resistance to these attacks must be continuously monitored and improved. Still, the mechanisms of cryptographic protection are widely used in the practice [1].

In practice, cryptographic protection is, as a rule, used for the ciphering and authentication of messages. Ciphering is a transformation of the message into an unintelligible form by a parameter that is called the cipher key. This parameter can be secret or public. The inverse transformation of the message can be performed by a secret parameter only, which is called the decipher key. Thus, we can keep the content of transmitted messages secret by ciphering these messages.

Authentication is the verification of the originality of the data delivered. It is based on the ciphering of data by a secret key and subsequent deciphering of delivered data by the respective public key. By authentication, we can verify whether the information itself or time data have not been modified and whether a given sender has really sent these data.

Modern cryptographic devices are able to ensure a high degree of confidentiality and authentication of transmitted data. Contemporary encryptors can cipher at rates in the order of units of Gb/s [2] and offer a wide spectrum of various types (end-to-end encryptors, network encryptors, link encryptors). We can realise cryptographic devices as software or hardware on different platforms [3]. The cost of their implementation is relatively quite low already and it continues falling. There are sufficiently good methods of key management too.

At present, various types cryptographic protections are used, which are implemented into terminals as a rule. The biggest advantage of this solution is the fact that the users can choose the quality of protection according to their requirements. The problem is it that potential attackers can connect themselves to the telecommunication network, they can monitor the network traffic, they can perform an analysis of both the ciphered and service traffic, they can modify the service traffic and they can impersonate some user or some element of the telecommunication network. These possibilities permit them to execute successfully different attacks on the overall security of the system or also on the cryptographic protection between terminals [4].

Manuscript received October 5, 2025
Manuscript revised October 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.10.14

3. Complex cryptographic protection

The contemporary development in the area of wireless local networks indicates a new trend, when the cryptographic protection is used not only between two terminals but also between the terminal and an access point to the network [4]. Only authorised terminals can be connected to the network, whereby the overall security is greatly increased.

Because of the decreasing cost of cryptographic protection, it is realistic to extend the concept of cryptographic protection in the access network to the entire telecommunication network. Then, the each element of the telecommunication network will be equipped with its own cryptographic protection. We will call the proposed concept the complex cryptographic protection of a telecommunication network.

As mentioned above, each element of the telecommunication network (e.g. switch, link termination, radio station, etc.) will be equipped with its own cryptographic protection. This protection will consist of three components (see Fig. 1):

1. the cryptographic control unit (CCU),
2. the encryptor/decryptor for each port of the given network element (PED),
3. the protection system against an unauthorised physical intrusion into the network element (PSP).

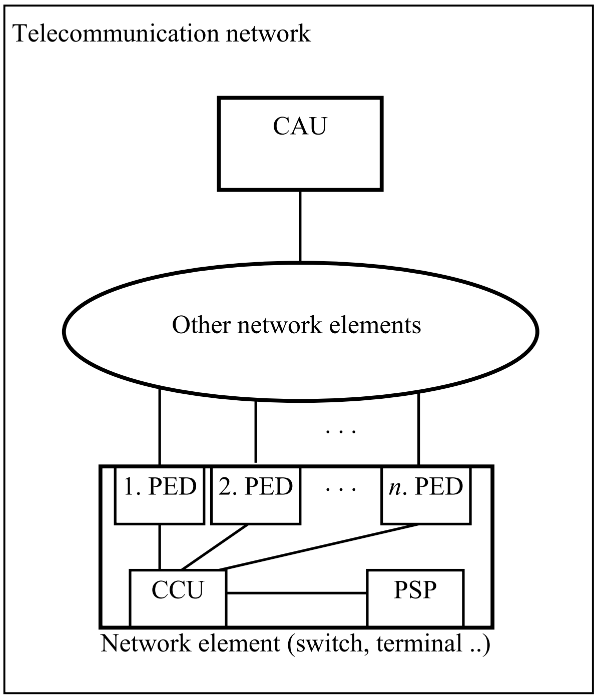
Telecommunication network
CAU
Other network elements
. . .
1. PED
2. PED
. . .
n. PED
CCU
PSP
Network element (switch, terminal ..)

Fig. 1 Cryptographic protection of a network element.

The cryptographic control unit CCU ensures the control of cryptographic protection of a given network element. It will realise the mutual authentication with other connected elements through the ports of the element. These authentications will ensure that no unauthorised element can be connected to the network. Thus, potential attackers can only perform the monitoring of the ciphered traffic between network elements. The cryptography control unit will ensure the keys for encryptors of the element and the security audit of the entire element.

Authentication for the whole network will be hierarchical. The central element of the network authentication system will be the central authentication unit CAU. All elements of the network control centre will be authenticated with respect to this unit. Through these elements other subordinated network elements will be authenticated and so on to the last network element.

Encryptors and decryptors on each port (PED) of the network element ensure the confidentiality of all transmitted data inclusive of the service data. In this way, the attackers lose the possibility to perform the traffic analysis and they cannot monitor or modify the service data.

The protection system against an unauthorised physical intrusion (PSP) into the network element prevents the attackers from obtaining from the given element keys and other cryptography data. In the case of a violent intrusion into the network element, the cryptography control unit erases the keys, performs the audit record and sends the information about the intrusion to the central authentication unit of the network.

4. Conclusion

At present, the described complex cryptographic protection of telecommunication networks offers a real possibility how to increase substantially the security of telecommunication networks.

The proposed concept also enables increasing substantially the security of large electronic systems that use these networks.

The concept increases the security of the cryptographic protection between terminals too, because the attackers must first overcome the network cryptographic protection and only then they can attack the cryptographic protection between terminals.

The weightiest open problem of the complex cryptographic protection of telecommunication networks is the requirement to establish new transmission standards. The service data needed for a correct operation of encryptors and for continuous authentication of transmitted data will have to be included in the transmission protocols.

References

[1] B. Schneier: Applied Cryptography. Wiley, N. York 1995.

[2] S. Trimberger, et al.: A 12 Gbps DES Encryptor / Decryptor Core in an FPGA. In: Lecture Notes in Computer Science, Volume 1965/2000, Springer-Verlag 2000, pp. 156-163.

[3] J. Nechvatal et al.: Report on the Development of the Advanced Encryption Standard (AES). National Institute of Standards and Technology, Gaithersburg 2000.

[4] T. Karygiannis - L. Owens: Wireless Network Security 802.11, Bluetooth and Handheld Devices. (SP 800-48). National Institute of Standards and Technology, Gaithersburg 2002.

Karel Burda received the M.S. and PhD. degrees in Electrical Engineering from the Liptovsky Mikulas Military Academy in 1981 and 1988, respectively. During 1988-2004, he was a lecturer in two military academies. At present, he works at Brno University of Technology. His current research interests include the security of information systems and cryptology.