On The Cryptographic Security Architecture of Czech Army Information Systems

Karel Burda
karel.burda@vabo.cz

Department of Communication Systems Management
Military Academy
Brno, Czech Republic

Abstract

At present, the requirements for the security of information systems are increasing. Modern cryptography provides not only for information confidentiality but also for authentication and information integrity. Simultaneously, the assortment of cryptographic protection products is extensive and prices are decreasing. These facts essentially change the importance and range of cryptographic applications in information systems.

Keywords: information system, cryptographic protection.

1. Introduction

At present, many information systems (IS) are introduced in the Czech Army (e.g. staff IS, logistic IS, etc.). These systems are spatially large and their elements can be anywhere in the Czech Republic. The plan is to build new computer networks for these information systems. The computer wide area network of the Czech Army (so-called: ”CADS”) will be the basic communication system for strategic information systems. The computer tactical network (so-called: “TAKOM”) will be the basic communication system for tactical information systems.

Cryptographic technologies must be used in information systems for secure transmission and storage of classified information. At present, requirements for the security of information systems are increasing. Modern cryptography provides not only information confidentiality but also authentication and information integrity. Simultaneously, the assortment of cryptographic protections is extensive and prices of the cryptographic products are decreasing. These facts essentially change the importance and range of cryptographic applications in information systems. Therefore there are many open problems regarding the cryptographic security of modern information systems. One of these problems is the following: What is the most suitable place for the implementation of cryptographic protects in information system architecture? This paper deals with this problem.

In this paper, the draft of the cryptographic security architecture for Czech Army information systems is proposed. In the first part of the paper, the Open Systems Interconnection (OSI) reference model and cryptographic protections in its single layers are briefly described. In the second part, the draft of the cryptographic security architecture for Czech Army information systems is proposed. This architecture is specified for strategic information systems and for tactical information systems. In conclusion, a brief summary is performed and recommendations for the introduction of cryptographic technologies in Czech Army information systems are given.

2. Cryptography and the OSI model

The International Organization for Standardization (ISO) standardized a reference model (ISO 7498) for the exchange of information between computer systems. This model is called the OSI (Open Systems Interconnection) model.

The OSI model consists of these layers [1]:

7 Application layer executes information processing.

6 Presentation layer defines data formats.

5 Session layer organizes data communication between remote applications.

4 Transport layer ensures the error-free transport of data through a transmission network.

3 Network layer organizes the transport route of data through a transmission network.

2 Link layer organizes the error-free transport of data through a transmission link.

1 Physical layer ensures the symbol transmission through a transmission link.

A cryptographic protection of the data is possible in any of these layers. The data processing is executed in the application layer. On the ground of software simplicity and cryptographic unification, it is better when cryptographic protection is solved in the lower layers. The presentation layer is responsible for the transmission format. It provides code conversion, data compression and data encryption. This layer is primarily designated for cryptographic protection of the data.

The next layer is the session layer. This layer is responsible for the initialization, maintenance and termination of the communication. For example, the cryptographic protection in this layer is realized by the protocol, SSL (Secure Sockets Layer) [2]. This protocol is designed for secure communication between client-server applications through the Internet. The SSL layer realizes the SSL protocol. From the point of view of the OSI model, the SSL layer includes both the presentation layer and the session layer. The SSL layer consists of two partial protocols - SSL Record protocol and SSL Handshake protocol.

The SSL Handshake protocol ensures the mutual authentication of a communication pair and the agreement of encryption parameters. We can see that this partial protocol matches with the session layer. The SSL Record protocol fragments, compresses and authenticates the data. These data blocks are encrypted and sent to the transport layer. On the opposite side, the received data is decrypted, verified, decompressed and data blocks are integrated. This protocol matches with the presentation layer.

The transportation layer ensures the data transmission between communication terminals. The security in this layer is generally solved by the recommendation X.273 - Network layer security protocol. Matters of data integrity, encryption, authentication and access control are described here. But this recommendation is too little known. For the Internet, especially, the security in the transportation layer is solved by the recommendation RFC 2246 - Transport Layer Security (TLS) protocol. But this protocol is the transport protocol according to its title, only, because TLS protocol, practically speaking, is the protocol SSL.

The network layer ensures the route of data through the network. The most popular security protocol in this layer is IPSec protocol [3]. This protocol is designed to solve the problems of data integrity and confidentiality on the Internet. Data integrity is ensured by the Authentication Header (AH) protocol. The data confidentiality is ensured by the Encapsulating Security Payload (ESP) protocol. In the network layer, data is placed into packets. In addition to data, the packets contain the block of control information (so-called: ”header”). Network devices transfer the packets from a sender to a receiver according to the information from the header.

AH protocol ensures data integrity. First, the original packet is hashed according to a secret key. This hash (so-called: ”authentication header”) is inserted in the original packet. This modified packet is transmitted to the receiver. The receiver excludes the authentication header and the packet hashes according to a secret key. The result must be the same as the authentication header.

ESP protocol ensures data confidentiality. First, the packets of data are encrypted and filed in the control information (so-called: ”ESP header”). This data block is hashed according to a secret key and the hash (authentication header) is added to the data block. In the end, the original packet header is appended and the modified data packet is transmitted to the receiver. The receiver authenticates the packet and decrypts the data.

Both AH and ESP protocol have two modes - transport mode and tunnel mode. In the case of the transport mode, the header of the authenticated or encrypted packet is the same as the original packet header. In the case of the tunnel mode, the authentication or encryption is performed, including the original packet header. Therefore, a special header is added to the authenticated or encrypted packet. This header makes it possible to address the transit or destination security gateway.

The link layer ensures the error-free transport of data through a transmission link. Cryptographic protections are not used in this layer. The physical layer ensures the transport of data symbols through a transmission link. Transmission devices perform the cryptographic protection in this layer. This protection is transparent for the higher layers and disallows traffic analysis. Not only payload but also control information is encrypted.

3. Cryptographic security architecture

From previous analysis, we can suggest the following recommendations for the implementation of cryptographic technologies in Czech Army information systems (in detail [4]). First, we suggest recommendations for strategic information systems (SIS).

It is optimal when cryptographic protections are situated as close as possible to the information source and the information sink - i.e., as close as possible to the application layer. Therefore, the cryptographic protections should be situated in the presentation and session layer. The presentation layer will ensure the confidentiality and credibility of the information (i.e., the encryption, decryption and data authentication). The session layer will be responsible for access control to the presentation layer (i.e., it will provide the authentication of the communication opposite). The session layer will also ensure the key agreements or key exchanges.

The encryption in the transport, network or link layer does not appear to be a good idea. The transmission protocols vary relatively fast (e.g. X.25 $\rightarrow$ TCP/IP $\rightarrow$ ATM $\rightarrow$?). For any new transmission technology it is necessary to solve the security of the information system again. This is expensive and complicated.

The encryption in the transmission devices (i.e. in the physical layer) is proposed but is not urgent at present. The presentation layer will ensure the confidentiality and the traffic analysis is not currently an adequate risk for strategic information systems.

The cryptographic protection may be realized by software or hardware technology. The software solution is cheap, good-class and sufficiently high-speed. It will be adequate for many applications in the Czech Army. The development of the software cryptographic protection must respect the future standards (e.g. P-1363) and must be accomplished together with the development of the secure operation system. The hardware cryptographic protection will be dedicated for applications with high demands on security.

The cryptographic security architecture according to these considerations is seen in Fig. 1. The computers with a cryptographic kit (PC_1 till PC_3) are connected to local area networks (LAN). These LANs are connected to the security gateway (SG) of the given organization. Security gateways are connected through a wide area network (CADS). For example, let us say that there is a need to transfer data from PC_2 to PC_3. First, the computer PC_2 begins the communication with the computer PC_3. Then mutual authentication is accomplished and the session key is established or transferred. The PC_2 encrypts and sends the data that the PC_3 receives and decrypts. During complete transmission from PC_2 to PC_3, the data always has the encrypted form.

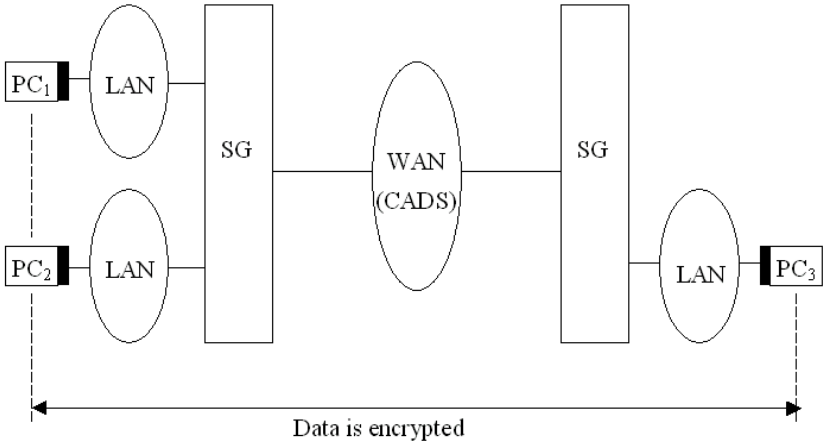

Figure 1. A draft of the cryptographic security architecture for strategic information systems.

We will now suggest recommendations for tactical information systems (TIS). The most important requirement of these systems is the restraint of the traffic analysis. An opponent can determine our battle formation from the control information in packet headers. Therefore, the necessary requirement for tactical information systems is the implementation of the cryptographic protections in the physical layer. Only the encryption in transmission devices forbids an opponent from executing a traffic analysis. For the development of tactical transmission devices, it is needful to join the development of cryptographic protections (so-called: "COMSEC") with the development of transmission protections (so-called: "TRANSEC").

The information in tactical information systems goes out quickly, so we don't need strong cryptographic protection. A protection in the physical layer will be adequate for many applications. The authentication of the communication opposite and the key agreements or key exchanges will be accomplished only occasionally (e.g., before a new mission). The protection in the presentation and session layer will be mandatory in information systems with higher requirements of data security (e.g., a cooperation between SIS and TIS). In this case, cryptographic kits for computers in TIS and SIS will be the same.

The draft of the cryptographic architecture for tactical information systems is in Fig. 2. For lucidity, it is described only at the brigade and battalion level. The architecture for lower levels is the same as for the battalion level. In the figure, we can see the vehicle of the brigade commander. This vehicle is connected through the router (RT) to the LAN on the brigade command post. Two radios with integrated ciphers (RS) are in the brigade commanders' vehicle. The brigade commander communicates with his superior by radio RS_1. The second radio, RS_2, is for communication with battalion commanders. Both radios are connected to the router RT. The LAN on the brigade command post is connected to the tactical network (TAKOM) by a radio relay with an integrated cipher (RR). We can see that any data emitted from the command post is encrypted. In this way, the classified data will be in decrypted form at command posts or vehicles only. The more important classified data will be protected in computers with the cryptographic kit. In this case, the data will be guarded during complete transmission from the sender's computer to the receiver's computer.

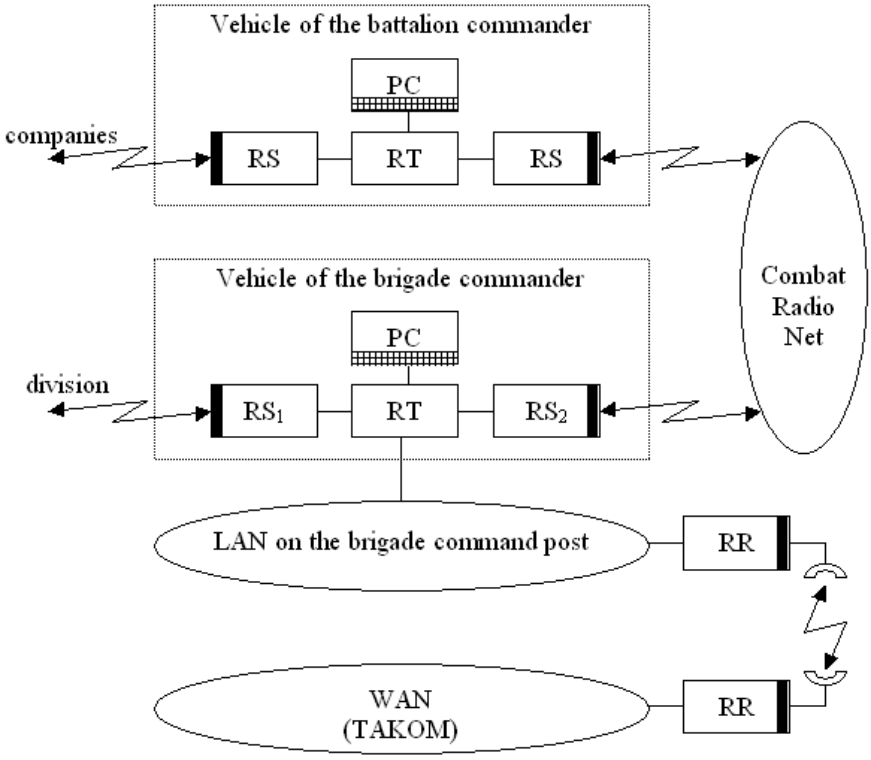

Figure 2. A draft of the cryptographic security architecture for tactical information systems.

4. Conclusions

Public key cryptography brings new possibilities for the security of communication and information systems. The main contribution of this cryptography is the digital signature, data authentication and authentication of the communication opposite. In this context, the public key infrastructure for the Czech Army must be planned and built with dispatch.

The cryptographic protection in the transport, network or link layer is not efficient. The transmission protocols vary relatively quickly. For any new transmission technology it is necessary to solve the security of the information system again. This is expensive and complicated, therefore it is useful to combine cryptographic protections in the presentation, session and physical layer.

For Czech Army strategic information systems, the cryptographic kits in individual servers and computers should ensure cryptographic protection. This protection should be implemented in the presentation and session layer. The cryptographic protection in the physical layer should be optional. The advantages and disadvantages of both the software and hardware cryptographic kits must be compared. The cryptographic kits should be developed simultaneously with the secure operation system.

For Czech Army tactical information systems, the information security should be ensured by the cryptographic protections in transmission devices (i.e. in the physical layer). A cryptographic protection in individual servers and computers should be optional. The protections in transmission devices should be developed simultaneously with the techniques of the transmission security (TRANSEC).

5. References

[1] Markley, R.W.: Data Communications and Interoperability, Prentice-Hall, Englewood Cliffs, 1990.

[2] OpenSSL project, www.openssl.org, 2001.

[3] Stallings, W.: IPv6: The new Internet protocol, www.comsoc.org/pubs/ surveys/stallings/stallings-orig.html, 1997.

[4] Burda, K.: Možnosti kryptografických ochran z pohledu modelu OSI pro komunikacní a informacní systémy ACR, VTÚE, Praha, 2000.