ISSN 0146-4116, Automatic Control and Computer Sciences, 2015, Vol. 49, No. 8, pp. 721–726. © Allerton Press, Inc., 2015.
Original Russian Text © A.S. Konoplev, 2015, published in Problemy Informatsionnoi Bezopasnosti. Komp'yuternye Sistemy.

Universal National Security Platform for Distributed Information and Telecommunication Systems

A. S. Konoplev

Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia
e-mail: artem.konoplev@ibks.ftk.spbstu.ru

Received May 8, 2015

Abstract—The problem of information security in distributed information and telecommunication systems has been considered. The paper analyzes the sources of threats in such systems. Existing security mechanisms have been examined. The class of threats associated with the use of untrusted (including imported) equipment is considered separately. The architecture of a universal security platform for distributed information and communication systems has been proposed.

Keywords: distributed ITCS, information security, backdoors, unauthorized access, data flow control, access control gateway

DOI: 10.3103/S0146411615080076

The continuous development of information technologies and the increasing demands for mobility lead to the promotion and the widespread introduction of information and telecommunication systems (ITCS) aimed at solving problems of distributed data processing, transmission of multimedia and telemetry data, and communication of users with each other. Requirements for the protection of transmitted and stored data, as well as organizations of the controlled access, are imposed on these systems.

There are the following sources of threats to information security in distributed ITCS (Fig. 1):

1. External intruders who, with the appropriate tools, can access the data processed in ITCS (by monitoring of the communication channel), change the message flow, block the operation of devices (by DoS/DDoS attacks), and introduce malware to end nodes of the system (through the exploitation of vulnerabilities in the system and application software of the terminal equipment).

2. Insiders who can establish unauthorized connections with the terminal equipment within the ITCS or outside of it, thereby making a data leak possible when processing various data.

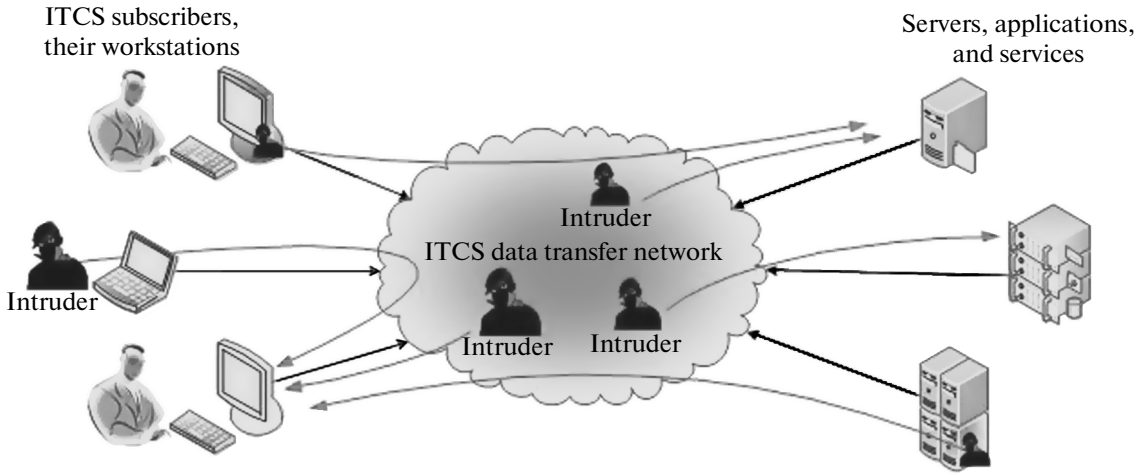

Fig. 1. Threats to information security in distributed ITCS.

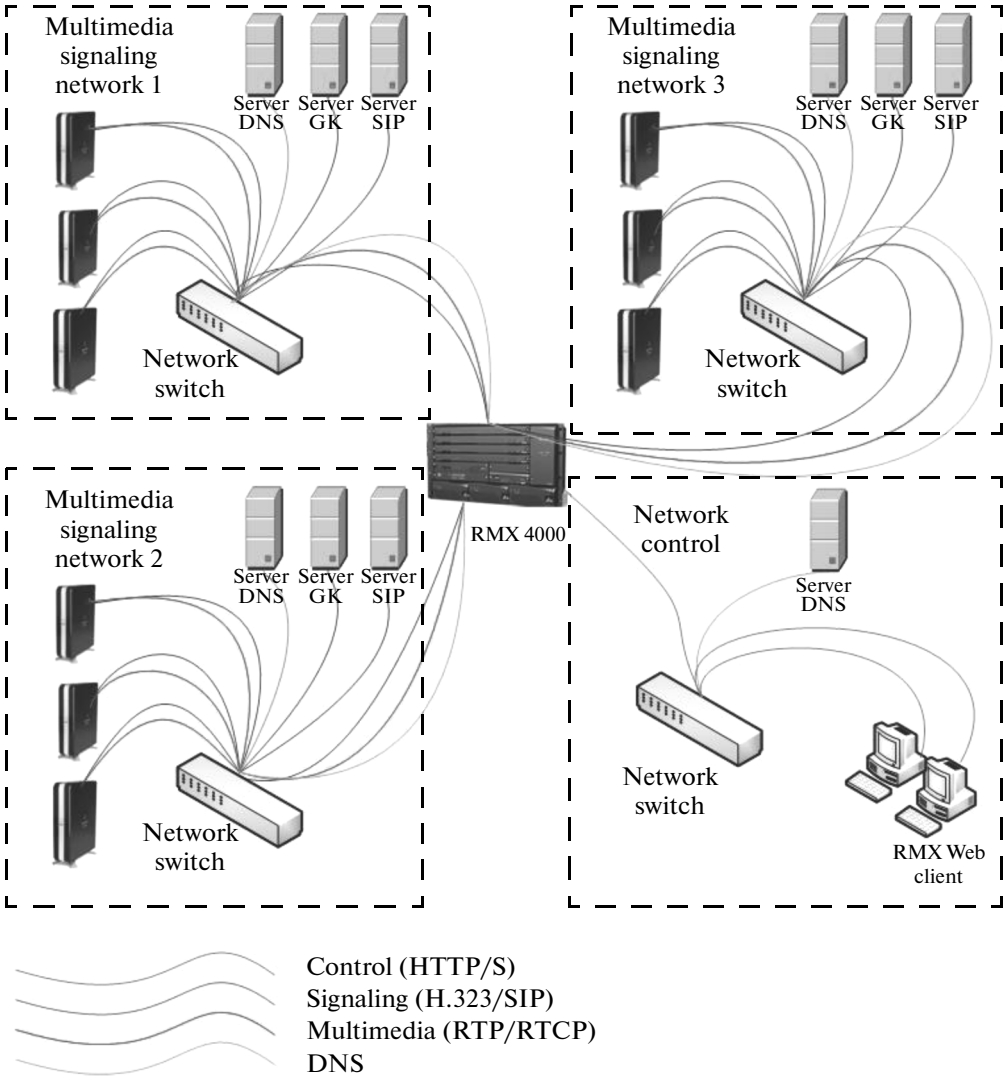

Fig. 2. The separation of networks of media, signaling, and control VoIP-networks.

3. Backdoors in ITCS equipment. This class of information security threats results from the use of untrusted equipment.

The use of encrypted communication networks in modern ITCS provides reliable protection from external intruders. At the same time, there is no method of protection against insiders that is as simple or universal. Functions of access control to data processed in the ITCS are partially implemented by software modules integrated by manufacturers in the technical means that ensure the ITCS operation. For example, the equipment used to organize networks for multimedia and telemetry data transmission (VoIP networks) can include software that has the following protection mechanisms:

—user authentication (including authentication with digital certificates);

—access control to the equipment in accordance with the role model (division of user accounts into operators and administrators);

—the use of white lists in determining legitimate network nodes;

—the encryption of multimedia traffic transmitted during communication sessions;

—the division of networks of multimedia, signaling, and control into separate subnets that makes it impossible for the intruder to control the equipment from the network that is not intended for control and to access the communication session from the network in order to control the terminal equipment (Fig. 2).

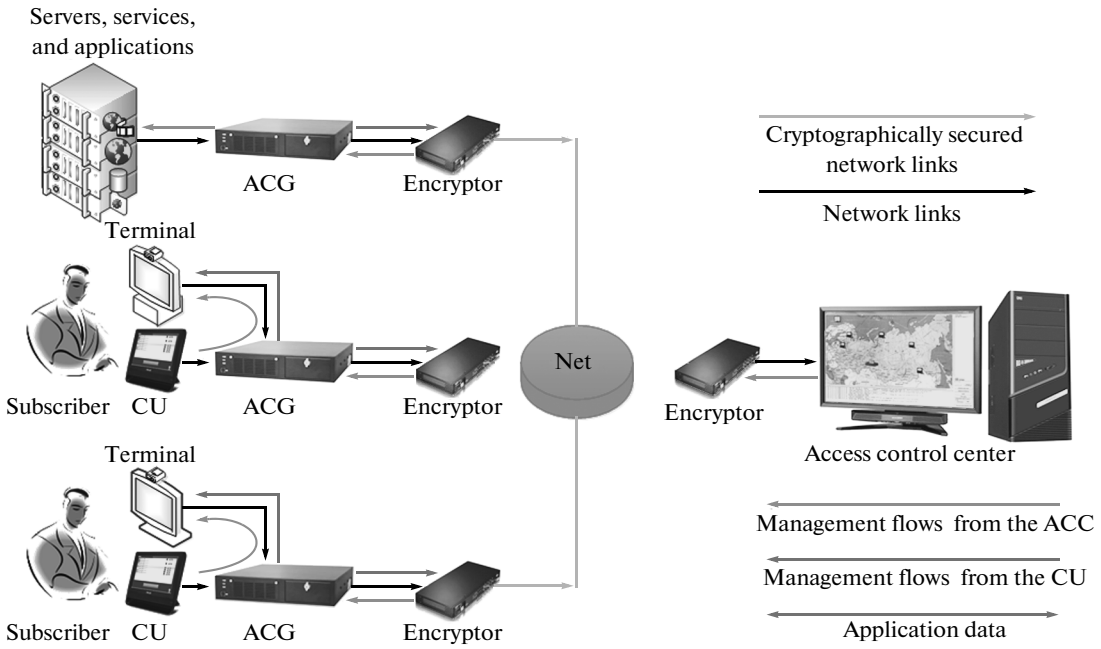

Fig. 3. The general structure of the secured distributed ITCS.

However, this equipment is generally manufactured abroad and uses untrusted software. For example, national video conferencing systems are in fact based on equipment made by Polycom, Tandberg and Cisco. This equipment becomes trusted only after certification procedures. Their mandatory requirement is that developers must provide software source code; in today's geopolitical situation, this is becoming impossible. As a result, the construction of secure ITCS must currently be accompanied by import substitution processes and the introduction of certified national protection mechanisms in them.

Under current conditions, the national platform based on the principle of distributed control of data flows that circulate in these systems can be used as a tool to ensure the security of distributed ITCS. Its purpose is to prevent unauthorized user access to network information resources and services including the one caused by backdoors and undocumented features in ITCS software and hardware.

The distributed control of data flows in the ITCS consists of monitoring and controlling the transmission of information between geographically distributed nodes of the system interconnected by the communication network. A time-limited mono- or bidirectional data interchange between two network nodes is understood under the data flow. In general, applications and services operating in the ITCS can require the data transmission between network nodes according to various schemes, i.e., directly, through a central hub, or by some other scheme. Thus, ITCS nodes form communication sessions by transmitting data flows according to a specific scheme. The information circulating within communication sessions is regarded as an access object.

In terms of architecture, the platform consists of the following components:

—The access control center that monitors, manages, and administrates the rules of the ITCS security policy.

—The access control gateway that acts as a means of differentiation and access control.

—The control unit used to authorize accesses by ITCS subscribers.

All of the aforementioned components of the distributed ITCS security platform are based on trusted hardware and software platform using certified national information security tools. The general structure of the distributed ITCS protected by the security platform is shown in Fig. 3.

Access Control Gateway (ACG) is the main component of the platform that monitors and controls access to information resources and services through the management of data flows within the network controlled network channel of the distributed ITCS. The main functions of the ACG are as follows:

1. The control of established network connections. Control consists of transmitting only the network traffic that is allowed to pass according to commutation rules and banning the passing traffic that is not explicitly allowed there.

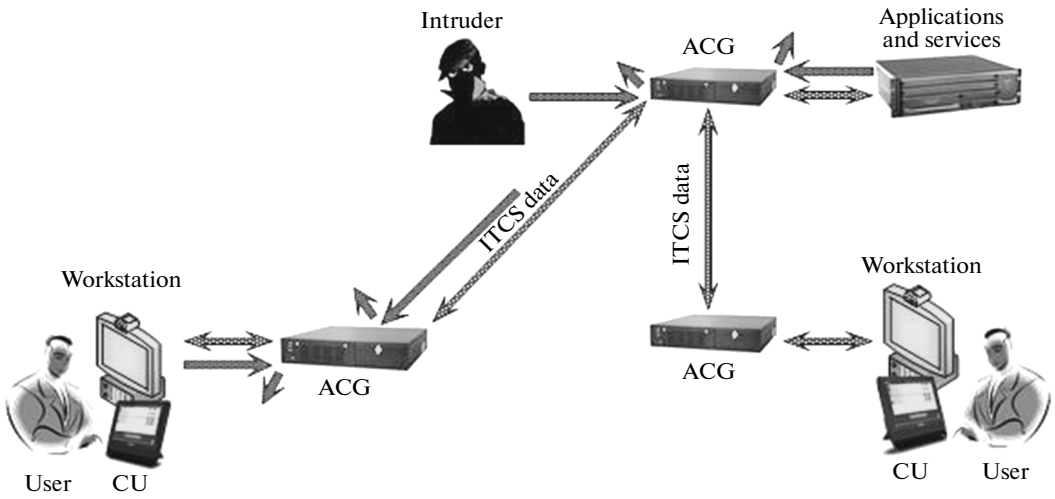

Fig. 4. Protection from security threats by means of ACG.

2. Monitoring and recording events. Events in the ACG are recorded during its operation in electronic audit logs. Information on changes of the state and ACG errors occurred during its operation is saved in the log of events. *State* refers to the set of settings of different ACG components, such as switching tables, switch configuration, and ACG network settings.

3. Data interchange with the access control center. The ACG collects and transfers data of the audit log and receives new switching tables.

4. The ACG is installed between the communication node and the ITCS network; it controls data transfers from the node to the network and vice versa, thus, allowing the transmission of only those data flows that correspond to the current security policy (Fig. 4).

In the security platform of the distributed ITCS, the ACG is responsible for the following tasks:

—blocking software and hardware input–output ports that are not involved in the execution of the objective function;

—the identification of interacting subscribers based MAC addresses and assigned IP addresses;

—monitoring the establishment of network connections in accordance with switching rules.

—restricting the access of ITCS subscribers to current connections in accordance with switching rules;

—blocking information leakage channels from one established connection to another;

—auditing events that occur in the ACG;

—operations of establishing and terminating network connections, as well as the forced shutdown of connections;

—changing the ACG configuration during operation.

The switch is the central ACG component, and it is responsible for the control of the switching of network nodes. Using the switching table that describes the allowed directions of data transfer in the form of IP addresses, the component decides on the further transmission of the packet in the network controlled by ACG or out of it. For each physical port, there is a list of allowed IP and MAC addresses.

The *access control center* (ACC) is the central node that controls a set of access control gateways and a computer network of the distributed ITCS. It is responsible for the collection of audit data, monitor of the state of nodes, and authorization of subscribers to resources and services of the protected distributed ITCS. The access permissions of subscribers to network resources are specified by the security policy.

The *security policy* is a set of rules stored in the ACC concerning restrictions and configuration data stored using the high level programming language that defines the allowable access operations for users with respect to the information resources and services of the distributed ITCS.

The *control unit* (CU) allows subscribers to control the terminal equipment of the ITCS and initiate the establishment of communication sessions. The CU is responsible for the network communication with other network components via the ACG.

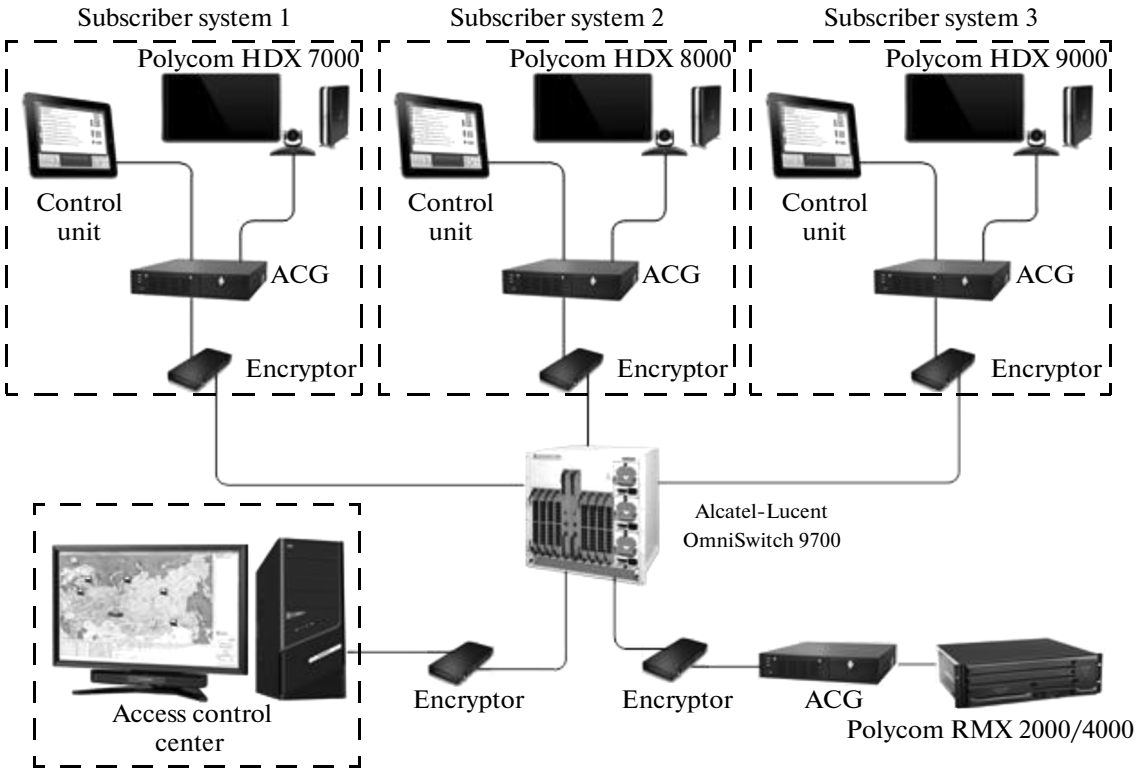

Fig. 5. The use of a universal security platform for distributed ITCS in videoconferencing systems.

The above approach to the construction of a universal national security platform of distributed ITCS was implemented as Kupidon system (certificate of state registration of computer programs no. 2009610136) for the control of data flows in protected distributed information systems built using IP networks of encrypted communication (Fig. 5).

The use of the Kupidon in modern distributed ITCS makes it possible to achieve the following objectives:

—to build an access control system without specification of the ITCS implementation;

—to ensure the effective protection of the ITCS from insiders when using untrusted and/or imported equipment;

—to implement centralized control of user privileges based on the system-wide security policy.

The versatility of the presented security platform makes it possible to use the Kupidon in such distributed ITCS as protected telecommunication systems of multimedia and telemetry data transmission (VoIP-based systems based on protocols H.323, SIP, etc.), protected distributed data processing systems (based on protocols FTP, HTTP, SMB, CIFS, POP3, SMTP, etc.), and protected distributed information systems (SOAP, SQL, RPC, etc.).

ACKNOWLEDGMENTS

This work was supported by the Ministry of Education and Science of the Russian Federation, project no. 2.1778.2014/K.

REFERENCES

1. Desnitskii, V.A. and Cheulin, A.A., The generalized model of the intruder and verification of information-telecommunication systems with embedded devices, *Tekhnicheskie nauki – ot teorii k praktike. Sb. st. po materialam XXXIX mezhdunar. nauch.-prakt. konf.* (Engineering: From Theory to Practice. Proc. XXXIX Int. Sci.-Pract. Conf.), Novosibirsk, 2014, no. 10 (35).
2. Zegzhda, D., Kalinin, M., and Savelyeva, O., The use of conference control to design a protected videoconference system, *International Conference on Enterprise Information Systems and Web Technologies,* 2008.

3. Konoplev, A.S., Zegzhda, D.P., and Kalinin, M.O., A secure system for centralized management of multiprotocol network equipment, *Sb. materialov XIX nauchno-tekhnicheskoi konferentsii "Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informatsii"* (Proc. XIX Sci.-Pract. Conf. Methods and Technical Tools of Information Security), St. Petersburg: Izd-vo Politekhn. Univ., 2010, pp. 103–104.
4. Konoplev, A.S., Zegzhda, D.P., and Kalinin, M.O., Centralized Management of Multiprotocol Network Equipment, *Sb. materialov XII Sankt-Peterburgskoi mezhdunarodnoi konferentsii "Regional'naya informatika (RI-2010)"* (Proc. XII St. Petersburg Int. Conf. Regional Informatics (RI-2010)), St. Petersburg: SPIIRAN, 2010.

Translated by O. Pismenov