N.D. Shukrullaevna

ENCRYPTION MEDICAL DATA BY SOFTWARE TRANSMISSION IN IP4 AND IP6 PROTOCOLS

(Department of Information Technologies, Tashkent University of Information Technologies Karshi branch, Karshi, Karshi-Beshkent yoli 3km, Uzbekistan)

Abstract. This article considers protection of medical data and information transfer for IP4 and IP6. Data protection in the global network has its own specifics, distinguishing it from the problem of information security in LANs. The most important feature of the problem of information security in the global network is the fact that the protection of the information is given entirely in software and hardware, and can not be solved by physically restricting user access to computers or hardware, as it can be done to limit access to information within a particular organization.

Keywords: Integrated Services Digital Network, General Packet Radio Service, Digital Imaging and Communications in Medicine, IP4 and IP6 protocols.

1 Introduction

In a global network of potential access to resources has any user, in any location on earth, and the time of access to the same or other information can not be predicted in advance [1-3]. Currently, telemedicine is widely used abroad, especially in the U.S. and Western Europe, where they already occupy a large segment of the general market videoconferencing . Initially, cost of equipment and operation of telemedicine systems was so great that they could afford only governments or oil companies. In the last five to ten years, with the development of national data networks , telemedicine systems have begun to progress and in the CIS countries, migrating from a purely scientific systems , serving , for example, human space flight, to the solution of applied problems in providing medical services to the population [2-3]. In Uzbekistan, telemedicine is a new area and waving, but while data security and protection of the health systems in science doesn't solved. Medical data differs from other data, they mainly in graphic or chemical form, the creation and protection of databases medical system difficult and complex task. Encryption - is the primary means of ensuring the confidentiality of information sent across the public data, including - on the Internet. Encryption can be used to protect any traffic, such as emails or downloads [2-3]. In addition, the encryption can protect information when it is stored, for example in databases that are on the computer, physical security which can not be provided (for example, an employee on a laptop on a business trip) . For encrypting the data communication channels using the same algorithms and programs as to create and verify digital signatures [2-3]. Again, the use of technology public key encryption requires each user to create private and public keys and their distribution. Public keys must be distributed and stored so that they are accessible to all users. In advanced applications can use digital certificates for Public Key certificates through the centers [2-3]. Pri-

vate keys are similar to passwords, and must be kept confidential by each user. Organization may decide that all employees were secret keys known to the leadership. User's private key must be stored as well as passwords. Report any suspected compromise of the private key, the user must immediately report to the security service [2-3].

2 Achieving this objective, the following tasks :

- Exploring telemedicine, compare the methods used with the new;
- Identify the scale and direction of development of information and communication technologies in telemedicine;
- Characterizing the external economic aspects of information security;
- Explore innovative methods in ICT, promoting and advancing the interests of safety;
- Analyzing and systematizing the international experience of using information technology to improve efficiency and safety on the example of the United States, the

European Union and China in this field;

- Identify urgent tasks for effective information security in telemedicine;
- Justify priorities and prospects for greater information security in the further integration of telemedicine into the world of globalization [1-4].

3 Encryption model of transmission medical data

3.1 Rules and facts of attacks related to subjective deliberate threats

A rule-based system is a knowledge-based system where the knowledge base is represented in the form of a set, or sets, of *rules*. Rules are an elegant, expressive, straightforward, and flexible means of expressing knowledge [7]. The simplest type of rule is called a *production rule* and takes the form:

IF <condition> THEN <conclusion>

In order for rules to be applied, and hence for a rule-based system to be of any use, the system will need to have access to *facts*. Facts are unconditional statements which are assumed to be correct at the time that they are used.

/ Rule1. */*

IF Attacks related to subjective deliberate threats
THEN system begin attacking situation

Facts can be thought of as special rules, where the condition part is always true. Therefore, the fact *Attacks related to subjective deliberate threats* could also be thought of as a rule:

IF TRUE THEN Attacks related to subjective deliberate threats

because have threat of attack.

/ Rule2. */*

IF Physical destruction of the system THEN system must protect medical data

/ Rule2.1 */*

IF Disabling or disabling the operation of the subsystems of computer systems THEN automatic turn on

/ Rule2.2 */*

IF began introduction of agents in the system personnel THEN automatic turn on

/ Rule2.2 */*

IF Interception of data transmitted through the communication channels, their analysis in order to determine the protocols, rules of entry into the network, and user authentication, and the subsequent attempt to simulate the penetration of the system THEN system reply who, when, where attacking

/ Rule2.3 */*

IF Theft of media (magnetic disks, tapes, memory chips, memory, and the whole PC); THEN declare attack and must work expert system.

/ Rule2.4 */*

IF Interception of data transmitted through the communication channels, their analysis in order to determine the protocols, rules of entry into the network, and user authentication, and the subsequent attempt to simulate the penetration of the system ; THEN after testing find out where broken parts of medical system.

4 Expected results consist of

- The practical importance of data protection;
- Registration of the patient passport data in its own database
- Registration, accumulation and storage in a database of digital X-ray images
- Maintains a database of X-ray images, which allows you to report, sort, and retrieve information on patient's name, type of study.
- Export images in accumulated other information systems in the format DICOM and HL-7 (e.g. for transmission over networks Internet / Intranet for international standard storage and transmission of medical images for teleconferencing, seek advice from the experts and operational training to receive the patient).
- Save images to a file format BMP, TIFF and JPEG.
- Preparation of patient data in electronic form in accordance with the requirements; • Direction of patient data, according to the list of indications for consultation body.

5 Conclusion

This paper presented encryption model of transmission medical data and rules and facts of attacks related to subjective deliberate threats. This model is the construction and design of expert systems for telemedicine networks and medical data leakage channel. System algorithm rules and facts of attacks related to subjective deliberate threats are based on theoretical and practical facts.

References

1. Review of ICT development in Uzbekistan 2006-2008, ICTP_Review_2008_RU_part_07.

2. Fundamentals of Information Security. Textbook for universities/ E.B.Belov, V.P.Los, Mesch R.V. Mershyakov, A.A. Shelupanov. -M.: 2006. - 544

3. S.V. Vikhorev, R.Y. Kobtsev "How to identify the sources of threats ?" / / Open Systems 7-8/2002, number. http://www.elvis.ru/files/howto.pdf.

4. "ENCODINGS OF MEDICAL DATA BY SOFTWARE TRANSMISSION TO OPEN COMMUNICATION LINKS OF VIPNET", Collection:- Mathematics, science, science in the economy and in society "(MIESEKO 2014), Moscow December 31, 2014.

5. www.mednet.ru. 6. www.wikipedia.org/wiki/IPv6.

6. Hopgood, Adrian A. Intelligent systems for engineers and scientists / Adrian A. Hopgood.--2nd ed. CRC Press Boca Raton London New York Washington, D.C.2000, 34- 49 pp.

D. Nurjabova

APPLICATION OF NEW METHODS AND METHODS CYBER CRIMINALISTICS

(Tashkent University of Information Technologies Karshi brnach,department"Software Engineering"
Shukurova Markhabo Tashkent University of Information Technologies Karshi brnach,department"Information technologies")

Abstract. This article is devoted to application of new methods and methods cyber criminalistics. Problems of cybercrime are considered in this article and given new methods .

Key words: cyber, criminalistics, cybercrime.

We live in the information space. I can not say exactly how this information closer to reality or engage in fraud on the Internet, hacking passwords large company sites or e-mail to threaten a person's life on the Internet, engage in hacking and other place around us every second growing cybercrime. What is cybercrime, and when there was this term in the Criminal Code. Computer security experts are well aware of the term and know what kinds of threats are struggling with them and define the concept of cybercrime.