CyberSecurity Concept For New Generation Telecommunication Networks

Nikolay Ulpe
JSC InfoCES
Moscow, Russia

Sergey Melnik
Moscow Technical University of Communications and Informatics (MTUCI)
Central Science Research Telecommunication Institute (CSRTI)
Moscow, Russia
sv.melnik@bk.ru

Abstract. **The article describes the main perspective directions of development of Worldwide network. Potentially number of connections to the Internet will increase to 70 trillion by 2025, reconstruction and modernization of modern communication networks and new approach to ensuring information security. Information security becomes a cornerstone of creation of communication networks of future generations and how data and communication networks will be protected safety of Society and State will depend. If today objects, potentially vulnerable from the Internet, are computers and the maximum harm which hacker attack can cause is a temporary suspension of work of automated control systems and access to information, any element of Digital economy can become object of attack in networks of the Industrial Internet of things. It is necessary for prevention of potential threats: to classify these threats; to have the uniform formal description of threats and the warning and correcting influence; to have the uniform concept of the organization of information security. This article brings up questions which creation of the uniform concept of information security of Russia with the purpose to minimize potential danger of harmful impact on significant objects of protection has to form the basis and to exclude possibility of network attacks to critical objects.**

Key words: **Internet, Security, IoT, IIoE, IoE, 5G, Modeling, Timing.**

VIII. INTRODUCTION

Internet of Everything (IoE) is the new concept for information exchange in telecommunication networks. This concept includes all main fields: Internet of Tings (IoT), Industrial Internet of Tings (IIoT) and Human data exchange networking. It is not only data exchange between any probes and big data centre. It is very important to have sufficient type approval and cyber security mechanism for this new concept. The report consists of the universal incident object description exchange format based on Recommendation ITU-T X.1541. This method describes all possible incidents based on standard classes. This is the basement for cyber security modeling and building new protected software solutions for secure data exchange. We used 27 basic classes ITU-T X.1541.

It is well understood that more and more devices are connected to worldwide network the Internet every year. If today the majority of connections corresponds to the animated users, i.e. the main sources of data are people, in the near future inanimate objects will become the main sources. For a long time networks of intermachine interaction of M2M which are gradually built according to requirements to creation of networks of the Internet of Thing (IoT) develop. In parallel there is a development of the uniform principles of remote control of important objects of infrastructure according to requirements of creation of networks of the Industrial Internet of prophetic (IIoT). Development in the field of the tactile Internet (TIoT) became more active in the latest time. For each of these directions it is required to establish necessary and sufficient measures for information security.

The Internet of Everything (IoE) or the General Internet is the new concept of exchange of information in communication networks including all above-named directions in total with information from subscribers of a communication network.

The main principles when determining measures of ensuring information security are:

- ranking of information sources;
- classification of protected objects;
- the uniform formal description of the threats arising in case of unauthorized access to information and in case of malicious change of information;
- the uniform formal description of the influence preventing unauthorized access and change of information;
- the uniform formal description of the influence correcting the unauthorized access taking place and change of information.

Extensive works on standardization are conducted for the purpose of ensuring uniform approach to information security. The main organizations which carry out these works are:

- International union of Telecommunication (ITU-T);
- International organization for standardization (ISO);

- Cloud Security Alliance (CSA), the organization of information security for cloudy structures..

Networks of the Internet of things unite a large number of the various sensors communicating on the public Internet. Security of objects of networks of the IoT has a class low and average. Networks of IIoT make the objects relating to infrastructure of digital economy. Security of objects of networks of the IIoT has a high class. Objects of the tactile Internet is an opportunity to feel the object which is at distance. Sensors which transfer its characteristics which are reproduced on the reception end are connected to object and create effect of a touch. Such mechanisms are used, for example, at remote inspection of the patient in a telemedicine. In its current stage of development there are devices for carrying out remote operations.

Considering high responsibility at information transfer, it is necessary to provide mechanisms of a guarantee of appropriate information security in future General Internet already today. The international standards in the field of cybersafety are developed and worked.

In Russia works on creation of standards for voluntary certification of objects of information security which have to become part of the uniform concept are also conducted.

II. INFORMATION SECURITY STANDARDIZATION

Groups of scientists and engineers worldwide work today on ensuring information security for IoT/IIoT/TIoT. In the field of information security treat the main aspects of standardization:

- risks assessment;
- general description of information on incidents;
- Web applications protection;
- detection of anomalies in a network traffic, "botnet" detection/protection;
- application of metrics and indexes for assessment of threats and measures of protection.

The main standards in the field of information security of IoT are developed in the International Union of Telecommunication (ITU-T), the research commissions (SG 13, SG17), in Cloud Security Alliance (CSA) and in ISO/IEC - research committee JTC1 SWG 5 and the SC 27.WG2 working group. There are general activities of the research commission of SG17 Q4 "Cyber security".

III. CYBEX METHODOLOGY (STRUCTURED CYBERSECURITY EXCHANGE, X.1500)

The principle of the organization of the protected data exchange between consumers is the cornerstone of counteraction to threats of information security. This exchange is specified by the recommendation of ITU-T X.1500 [1].

The methodology of Structured Cybersecurity Exchange (CYBEX) is developed for the protected data exchange between consumers. The methodology of CYBEX represents the five-level block model of data exchange shown in figure 1.

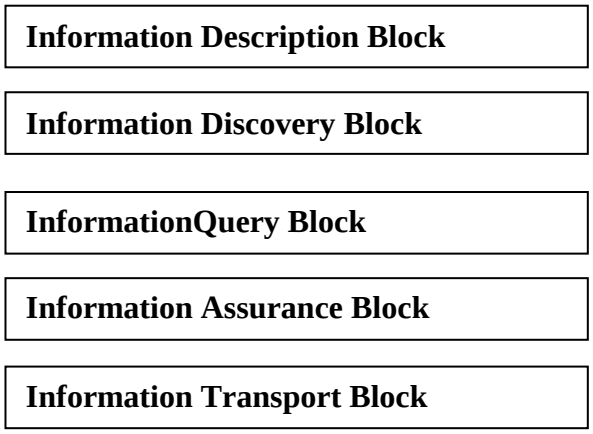

Fig. 1. Functional CYBEX blocks

IV. INFORMATION DESCRIPTION BLOCK

This functional description of information which is required to be transferred between consumers includes a format and language of the description. Formats and languages of the description information are provided in 21 international standards [2]. Standards of the block of the description of information include components on:

- format of the description of vulnerabilities of CVE – X.1520 [4];
- the catalog of descriptions of threats of CWE – X.1524 [5];
- format of the description of the CPE platforms – X.1528 [6];
- metrics for the quantitative assessment of vulnerabilities of CVSS – X.1521 [7];
- the catalog of patterns of attacks and methods of protection of CAPEC – X.1544 [8];
- language of the description of criteria of the vulnerable software of OVAL – X.1526 [9];
- format of the description of incidents of computer safety of IODEF – X.1541 [10].

V. INFORMATION DISCOVERY BLOCK

This functional block is responsible for definition and research of information on a source. There are two paradigms such as centralized maintaining a database of the entrusted sources (OID [10]) and the decentralized mechanism. On the Internet both of these mechanisms are used. The centralized mechanism of maintaining a database of the entrusted sources is based on entering of information on safety into a special database. Each country has the digital identifier in OID. The OID 2.48 identifier is appropriated to the safe site.

Together with the centralized the decentralized method of identification of safe sources RDF World Wide Web Consortium (W3C) [11] is used. RDF works at a basis of own search algorithm includes a method of an automatic assessment of safety of sources.

The Countermeasure Knowledge Base accumulates information on countermeasures that corresponds to cyber risks. To describe information in the knowledge base, CYBEX introduces the Common Vulnerability Scoring System (CVSS), Common Weakness Scoring System (CWSS), Open Vulnerability and Assessment Language (OVAL), eXtensible Configuration Checklist Description Format (XCCDF).

The Product & Service Knowledge Base accumulates information on products and services. To describe information in this knowledge base, CYBEX introduces Common Platform Enumeration (CPE) and Common Configuration Enumeration (CCE). CPE provides a structured naming scheme for information technology systems, languages to describe it. These formats and languages are platforms, and packages, while CCE provides unique identifiers to system configuration issues to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. That knowledge on cyber risks and countermeasures are often linked to specific products and services. For instance, a CVE is linked to CPE identifiers and CVSS scores in NVD.

VI. INFORMATION QUERY BLOCK

The block of a query of CYBEX represents specially developed programming language of the protected inquiries of CYBEX X.chirp. The specification allows to use additional fields for providing and monitoring of parameters of information security in standard language of inquiries of SQL.

VII. INFORMATION ASSURANCE BLOCK

According to methodology of CYBEX, three standards for certification of the protected sources are provided: X.evcert, X.eaa and ETSI TS 102042 V2.0. The standards X.evcert, X.eaa describe the algorithms similar to a digital signature, with that difference that this signature (digital certificate) can be appropriated to automatically entrusted source. The ETSI TS 102042 V2.0 standard provides the mechanism of existence of the organization for certification which can carry out recognition of certificates of the sites of the public Internet under the responsibility. It describes these requirements for certification authorities issuing public key certificates.

VIII. INFORMATION TRANSPORT BLOCK

The block of transportation of information is based on the protocols standardized by X.cybex-tp. The general description of transport protocols of the protected information transfer is provided in the X.cybex-beep specification. Besides, there are protocols described in the ETSI TS102232-1 standard. All these protocols of the protected information transfer on the public Internet use means of cryptography (enciphering). Length of a code depends on the importance of information parcel and on the class of security, CYBEX defined in the block of the description of information.

Albeit other protocols can be used for this transport, currently only the BEEP protocols are being investigated. Other candidate protocols, such as SOAP, exist but no draft recommendation for such protocols have been presented yet. From the viewpoint of forensics, ETSI TS102232-1 is also introduced here. This provides assurance of forensics information delivery to law enforcement and security authorities.

IX. INFORMATION SECURITY ORGANIZATION

In general process of ensuring information security is based on maintaining automatically updated databases so-called “the entrusted sources”. The mechanism of the automated certification of sources works. Contents of the site and a stream of inquiries from it are analyzed by the special software then the site is brought in a database with assignment to it the certificate of a safe source [12].

Thus, development completely specialized, including domestic operating systems is unfairly expensive and a little effective. It is expedient to use the software with an open code (OpenSource). This approach is used today by all large corporations for creation of the systems which are a trade secret. Using Open source software, it is possible to apply all available libraries to interfaces, input-output of data, etc. and to concentrate forces and means only on development critical, from the point of view of the developed technology, procedures which code, naturally reveals to nobody.

Thus, it turns out to cut down significantly terms and expenses on development demanded, having at the same time increased its reliability, thanks to a large number of already debugged fragments. At that we should also add that it is much easier to find the programmers owning the means relating to group of an open code comparing those who owns highly specialized knowledge. Thus, if we want to organize production of the professional software, but not “garage programming”, this way is preferable.

X. TIMING FOR CYBER SEQURITY

For the mechanism of digital certification in the protected networks, the synchronous time scale and a binding to it of all inquiries and answers are used. For ensuring unity and accuracy of this process it is expedient to use Timinator, the new modular server of time of production (KOMCET). This product is intended for work in future networks of mobile communication 5G and has to become one of the most effective remedies of high-precision synchronization of time and frequency with use of GLONASS/GPS/COMPAS/GALILEO together with the high-precision built-in generator and implementation of the PTP protocol.

XI. ACKNOWLEDGMENT

It is necessary to develop the uniform concept of ensuring information security of the general Internet taking into account requirements of the international standards and standards of the legislation of the Russian Federation. This concept has to include classification of objects of protection, importance of potential threats and methods ensuring the actions preventing threats of information security in total with the correcting influence in case of realization of this or that threat.

It is necessary to develop system of voluntary certification in the field of ensuring information security and national standards for this system.

XII. REFERENCES

[1] Overview of cybersecurity information exchange. Recommendation ITU-T X.1500. 04/2011.

[2] Takahashi T., Kadobayashi Y., Fujiwara H. Ontological approach toward cybersecurity in cloud computing // Proceedings of the 3rd International Conference on Security of Information and Networks. 2010. P. 100–109.

[3] Common vulnerabilities and exposures. Recommendation ITU-T X.1520. 01/2014.

[4] Common weakness enumeration. Recommendation ITU-T X.1524. 03/2012.

[5] Common platform enumeration. Recommendation ITU-T X.1528. 09/2012.

[6] Common vulnerability scoring system 3.0. Recommendation ITU-T X.1521. 03/2016.

[7] Common attack pattern enumeration and classification. Recommendation ITU-T X.1544. 04/2013.

[8] Language for the open definition of vulnerabilities and for the assessment of a system state. Recommendation ITU-T X.1526. 01/2014.

[9] Incident object description exchange format. Recommendation ITU-T X.1541. 09/2012.

[10] International Telecommunication Union. Information technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree. X.660. August 2008.

[11] The World Wide Web Consortium (W3C). Resource Description Framework (RDF). 2010. URL: http://www.w3.org/RDF/.

[12] Tom C. Security and IoT in IEEE standards // IEEE-Standards, February 2016.