Nonlinear Phenomena in Complex Systems, vol. **17**, no. 3 (2014), pp. 210 - 214

Modern Problems of Cybersecurity

Y. S. Vasiliev and P. D. Zegzhda
Saint-Petersburg State Polytechnic University,
29 Politechnicheskaya Str, 195251 Saint-Petersburg, RUSSIA

V. I. Kuvshinov
Joint Institute for Power and Nuclear Researches "Sosny
99 Academician A. K. Krasin Str, Minsk, BELARUS

(Received 13 May, 2014)

Analysis of the basic tendencies of occurrence of new threats of safety is resulted. Characteristics of a postindustrial society is given. New problems of maintenance of cybersafety are formulated. Ordering of technological protection on the basis of the offered model is spent.

AMS Subject Classification: 68R10, 94C15
Keywords: cyber threats, dynamic protection, security model

1. Introduction

Post-industrial society is currently in a state of a permanent informational revolution, which is now at the stage of global computerization of industrial objects management systems and their integration into the Internet, which inevitably makes them more vulnerable to potential violators in terms of information security. The media reports new cyber crimes, system breaches and cyber attacks almost every week [1–3].Considering that the number of attacks constantly increases, their mechanisms are being automatized and automated control systems (including military and special ones) as well as data infrastructure depend considerably on electronic means of data access and transfer, even a minor attack may deal catastrophic damage. There are known cases of the modern IT that is considered malicious (viruses, cyber attacks) being used to exert aggressive influence on data infrastructure and automated military control systems of other countries [2].In addition, computerization of personal communication devices and household appliances made elements of a smart home a part of the global cyberspace. The modern era is characterized by total internetization of the society, the Internet becoming a universal environment that allows to transitively enclose all informational aspects of economics, politics and private life in a single cyberspace. Thus the notion of cybersecurity emerges, meaning the security of the cyberspace, that characterizes a new class of threats that exploit the transitivity of the connections to perform attacks or deliver the necessary tools [5,6]. So the advanced solutions in IT need to be constantly analyzed in order to forecast changes in the character of cybersecurity threats and to determine most promising and relevant course of research and developments in this field that would forestall the tendencies of threats evolution. The work experience in this field shows that attack and defense technologies are inseparably linked, and that a profound knowledge of methods and technologies used by the opposite side is essential for creation of an effective solution. An attempt to analyze the major tendencies in emergence of new security threats and their mechanisms allows us to recognize the following tendencies on the current technological level [4–7].

- Emergence of new types of cyber attacks that is characterized by the target object shift from data and programs to the management systems that is aimed at disabling industrial machinery information systems;

- The purpose of the contemporary attacks is to seize control and impose new operation algorithms on a target system;
- The attack becomes a planned cyber operation targeting a meticulously picked object and including stages of preparation, means of defense breach development and provision of the attack source secrecy;
- Mechanisms of malicious software distribution are constantly improving from searching for vulnerability and creating exploits to social engineering in social networks. The emergence of a specific "hacking of service" service in a form a website network and black hole-type software proves that the production of malicious software and its distribution has become a legitimate part of IT.

The contemporary cyber attacks with aforementioned features are called cyber threats [1, 7].They have the following distinctive features:

- Purposefulness of the attack even when it is performed transitively through intermediate nodes.
- A wide range of means to achieve the goal.
- Using supercomputers to create new attack scenarios, interfere with production management as well as in system scanning and cryptanalysis. Considering the beginning of the cyber warfare era, supercomputers can create new weaponry.
- Outsourcing developers to perform an attack.
- Fight for a control over the global cyberspace infrastructure.

Current situation creates new challenges for researchers and developers of cybersecurity methods, which is exactly the problem of providing cybersecurity and the subject of the present special issue. Today, the developers of methods to provide cybersecurity set the following tasks [5, 8–11]:

- Being one step ahead in the cyber arms race and development of cybersecurity technologies, recognizing the emergence and implementation of cyber threats beforehand, thus anticipating cyber crime and eliminating opportunities.
- Training IT staff of the safety-critical objects and informing customers in term of information security.
- Examining vulnerabilities as a new approach to assessing the level of security.
- Integrating IT and security means into protected automated control systems resistant to cyber attacks.
- Developing the virtualization technology as a powerful defense mechanism:
  - building protected platforms using virtualization technologies.
- Examining policy models of blurring perimeter systems, the Internet as well as security control and management in such systems.

The transition to cybersecurity creates the necessary prerequisites for the creation of a new paradigm of providing cybersecurity for the modern IT, which includes:

- Reviewing access management models that take into account openness, versatility and distribution of the modern IT systems.
- Recognizing the virtualization technologies as a powerful defense mechanism that creates a foundation for proving the isolation of one part of a system from the other, allowing to shift from the concept of a "protected system" (protected from a fixed number of threats) to the concept of a "system with predictable behavior".

- Implementing the principle of separating the data processing environment from the security tools.

- Creating theoretical background for dynamic security management (adapting to current threats) as an object of automatic management with a stability zone, aftereffect and dynamic characteristics.

- Developing an approach to assessing elasticity and scalability of the security system.

The urge towards automatizing security management to a maximum by adapting it to certain conditions and, eventually, to a stream of destabilizing factors plays a major role.

2. The evolution of information security paradigm

The analysis of existing tendencies allows making a retrospective conclusion considering the change of the information security paradigm. It can be conditionally defined as static, active, adaptive and dynamic security. Static security proceeds from identification of the most dangerous threats, countering action function, which are essential to be implemented, and ingress protection rating that the system must correspond to [12, 13]. The set of security functions has to correspond to the threats. The major drawback of this technology lies in limitation of the number of threats. If this number is expanded, it may lead to security vulnerability. Other security technologies involve more or less developed check system. It allows expanding the number of threats that security can handle, make multiple border security that allows developing the system by plugging in extra software or administrative measures aimed at security maintaining. The proposed systematization of security technologies is based on two main factors: available components for system reliability analysis and its operational environment; security criteria in use (see table 1 below). The articles provided herein reveal several issues of cybersecurity taking into account the provided tendencies and can be classified in the following way:

I The problems of theoretical cryptology aimed at the implementation of algebraic approach to the research of formal mathematical frameworks of cryptosystem engineering (see the papers “Strengthening differential and linear attacks using virtual isomorphisms”, “On boolean ideals and varieties with application to algebraic attacks”, “Analysis of hidden field equations cryptosystem over odd-characteristic fields” in this issue).

II The problems of network interaction security modeling on the basis of graphic charts and algebraic methods (see the papers “Dimension reduction in network attacks detection systems, “Efficiency evaluation of botnets’ disinfection and removal”, “Formal security model for virtual machine hypervisor in cloud systems”, “Formalization of objectives of Grid systems resources protection against Unauthorized Access”, “Reflexive control over intruder using deception systems”).

III The problems of theoretical cryptology aimed at the implementation of algebraic approach to the research of formal mathematical frameworks of cryptosystem engineering (see the papers “Strengthening differential and linear attacks using virtual isomorphisms”, “On boolean ideals and varieties with application to algebraic attacks”, “Analysis of hidden field equations cryptosystem over odd-characteristic fields” in this issue).

IV The development of approaches to the formalized evaluation of information system security and a set of adjacent issues (see the papers “Approach to assessment

Table 1: The characteristics of existing security technologies

Nature of security	Model 1			Evaluation methods of security	Main characteristics
	System status	Security system status	Interchange with environment		
Static	not available	not available	fractional	evaluation by requirements documents	Adequacy to threats
Active	fractional	not available	analysis of incoming information	analysis of information environment	Reliability of analysis of incoming information
Adaptive	fractional	fractional	analysis of incoming information	Security measures status monitoring	Threat tolerance, control stability
Dynamic	full	full	analysis of incoming information and communication pathways	system security monitoring, risk assessment	Security independence, resistance to weaknesses, sufficiency

of measures sufficiency of confidential information protection", "Using principles of fractal image compression for complexity estimation of the face recognition problem" in this issue).

References

[1] P.D. Zegzhda. Modern tendencies in development of methods and measures of confrontations in the Internet. In: *Book of XII All-Russian conference "Information security. Regional aspects. InfoBEREG - 2013"*, 10-15 September, 2013, Sochi.

[2] L. Melevski. Stuxnet and strategy: A special operation in cyberspace. Joint Force Quarterly. **63**, 64-69 (2011).

[3] R. Axelrod, R. Iliev. Timing of cyber conflict. [electronic resource]. http://www.pnas.org/cgi/doi/10.1073/pnas.1322638111

[4] V. Skormin. F. Schneider's view on cyber security science project. In: *6th International conference MMM-ACNS-2012, SPb, 2012.* (Springer, 2012). Pp. 22-35.

[5] P.D. Zegzhda. Trusted securing of environment resistant to cyber threats. Problems and perspectives. In: *Book of XVI national forum of information security "Infoforum - 2014"*, 30-31.01.2014, Moscow. P.2.

[6] F. Martinelli, I. Matteucci, Ch. Morisset. From Qualitative to Quantitative Enforcement of Security Policy. In: *6th International conference MMM-ACNS-2012, SPb, 2012.* (Springer, 2012). Also at http://comsec.spb.ru/mmm-acns12/openconf.php?menu=accepted

[7] *Trust in cyberspace by Fred Schneider.* (Natural academy press, Washington, 1999).

[8] P.D. Zegzhda, M.O. Kalinin. Automatic Computer Security Management. Problems of

information security. Computer systems journal. **4**, 15-23 (2013).

[9] P.D. Zegzhda. Strategy of dynamic security In: *Materials of international academic conference on security issues and counter-terrorist actions*, Moscow State University, 2-3 November, 2005. (Moscow, 2006). Pp.216-229.

[10] GOST R ISO/IEC 17799-2005. "Information technology. Working rules for information security control."

[11] GOST R ISO/IEC 27032-2012. "Information technology. Methods for providing security. Guidance for cybersecurity".

[12] A.L. Fradkov. *Cybernetical physics: from chaos to quantum control.* (Springer–Verlag, 2007).

[13] *Cybersecurity: Public Sector Threats and Responses.* Ed. Kim Andreasson. (CRCPress Taylor Fancies Group, LLC, 2012).