ISSN 1019-3316, Herald of the Russian Academy of Sciences, 2014, Vol. 84, No. 6, pp. 424–431. © Pleiades Publishing, Ltd., 2014.
Original Russian Text © I.V. Kotenko, I.B. Saenko, 2014, published in Vestnik Rossiiskoi Akademii Nauk, 2014, Vol. 84, No. 11, pp. 993–1001.

From the Researcher's Notebook

Scientific and technological progress generates two interrelated trends: new machinery and technologies, on the one hand, open unprecedented opportunities in all practical spheres and, on the other, provoke numerous negative consequences that are often impossible to predict in advance. This is also true of information and communication technologies, whose rapid development in the past decades has called into existence the dangerous phenomena of cyberterrorism and cyberwars. As is the case with other threats associated with the use of scientific and technological achievements, society responds with technological improvements. A specific example of such improvements within a pan-European research project with the participation of Russian scientists is given below.

DOI: 10.1134/S1019331614060033

Creating New-Generation Cybersecurity Monitoring and Management Systems

I. V. Kotenko and I. B. Saenko*

From 2010 through 2013, the Seventh EU Framework Program for Research and Technological Development was actively designing the architecture, models, methods, and operation algorithms for systems that monitor and manage the cybersecurity of information infrastructures. These studies were united in the Management of Security Information and Events in Service Infrastructures (MASSIF) project [1], in which groups of scientists and designers from Spain, Italy, France, Germany, Portugal, South Africa, and Russia took part. Our country was represented by a research team from the Laboratory of Computer Security Problems of the St. Petersburg Institute for Informatics and Automation, RAS (SPII RAS).

The studies were based on a security event and information management technology—a new intensively developing trend in cybersecurity with a large potential for detecting threats and generating countermeasures to ensure the required level of security for information infrastructures [2, 3]. The cybersecurity monitoring and management systems oriented at this technology require the operational collection, storage, and subsequent analysis of data about security-related events. Initially, these data are formed and fixed in the system logs of various hardware and software components of the computer infrastructure. These components are servers, workstations, routers, network firewalls, database management systems, intrusion detection systems, antivirus tools, etc. Such information protection systems can be called the first generation of security monitoring and management systems. They have been widely commercialized; however, the sphere of their application, as a rule, does not spread beyond information processes within computer networks. Today an increasingly urgent problem is the detection of cyberattacks and other malevolent actions not only at the level where the events registered in network logs are analyzed but also at the level of business processes, as well as information obtained by physical sensors. In addition, the well-known commercial security monitoring and management systems are facing serious challenges as they operate in large computer networks.

The above-mentioned drawbacks of the existing commercial security monitoring and management systems and several other problems have necessitated the MASSIF project aimed at building systems free from the specified drawbacks and defined as *new-generation cybersecurity monitoring and management systems*. This article generalizes the main results of the MASSIF project on the construction of such systems and considers the possible application scenarios for these developments.

TECHNOLOGICAL REQUIREMENTS AND THE MAIN SOLUTIONS

The technological necessity of creating new-generation cybersecurity monitoring and management systems is predetermined by the current trends in the development of information–communication technologies (ICTs), primarily associated with the support of distributed infrastructures oriented at wide use of the Internet. For contemporary ICTs, two paradigms have become flagship: the Future Internet and the Internet of Things. The first covers research projects aimed at developing new architectures for systems that actively use the global web, and the second represents a concept of building a computer network that unites

* The authors work at the Laboratory of Computer Security Problems at the St. Petersburg Institute for Informatics and Automation, RAS. Igor Vital'evich Kotenko, Dr. Sci. (Eng.), is head of the laboratory. Igor Borisovich Saenko, Dr. Sci. (Eng.), is a leading researcher.
e-mail: ivkote@comsec.spb.ru; ibsaen@comsec.spb.ru

physical objects ("things") capable of interacting with one another or with the environment primarily by the Internet. Both paradigms are event oriented; therefore, their implementation in information systems and infrastructures will have to solve new cybersecurity problems associated both with significantly increased systemic information flows, which circulate through the Internet, and with a sharp growth in the diversity of sensors and devices that disseminate security information via the Internet.

Another trend is the significantly increased role of intelligent methods and services of cybersecurity. They are the only possible instrument that helps process a large amount of information, which is necessary for making justified decisions on cybersecurity, and they ensure protection modeling and prediction, as well as the development of countermeasures and recommendations. All this should significantly improve the efficiency of cybersecurity.

The above information allows us to make two important conclusions on the future of cybersecurity monitoring and management systems. First, in the near future these systems will increase their magnitude because they are closest to the above-mentioned paradigms and are aimed at solving new problems of information security assurance. Second, the objectives of cybersecurity monitoring and management will become more complex, because they should affect distributed business processes under inaccessibility and/or possible unauthorized alteration of data. Therefore, the new-generation cybersecurity monitoring and management systems are designed to implement intelligent methods most fully and can be deployed as cloud-based services, when the assurance and confidentiality of security information are becoming especially urgent.

Thus, the technological need to create new-generation cybersecurity monitoring and management systems predetermines their orientation toward

• the development of reliable and stable means to ensure user awareness about security [1–4];

• the improvement of the distributed management of security for the adaptive configuration of security policies;

• attaining a higher scalability for the required productivity growth under an increased amount of processed data;

• the use of innovative models of security prediction, capable of proactive processing of security incidents and events; and

• the decentralization of security event acquisition and processing between central and remote components.

The complex of decisions on the creation of cybersecurity monitoring and management systems, developed within the MASSIF project, ensures implementation of the following new functional capabilities:

• the interlevel correlation of security events, incoming from various heterogeneous sources;

• adaptive and highly scalable event processing, ensuring the management of large amounts of security data in real time or with a minimal time lag;

• the prognostic analysis of security for the proactive detection and prevention of attacks by taking the corresponding countermeasures; and

• a high accessibility and resilience of security-event data retrieval under a territorially distributed protected infrastructure and an active and/or inadvertent attack on communication channels.

The generalized typical architecture of the new-generation cybersecurity monitoring and management system, proposed by the participants in the MASSIF project, is shown in Fig. 1. It has the following levels: network, data, events, and applications.

The *network level* includes data retrieval agents, which are represented by all sources that provide information about cybersecurity events, such as network devices, servers, workstations, databases, internetwork firewalls, antiviruses, and various sensors.

The components of the *data level* are a translator, designed to preprocess and convert security event data in line with the internal format, and command dispatch agents, which ensure the delivery of security decisions to remote infrastructural components.

The main component of the *event level* is a data bus, which is responsible for the dissemination of information about security events and their guaranteed delivery to the other system components.

The components of the *application level* include

• an event analysis component, which ensures adaptive support for all event-processing tasks and functions in real time;

• a security data repository, which contains detailed and generalized data delivered on requests to other components;

• a countermeasure selection component, which ensures the centralized verification and management of security policies to protect infrastructural components;

• a component that assesses the protection of an informational structure, which provides for additional analytical capabilities by implementing functions that model attacks and analyze protection; and

• a visualization component, designed to deliver security information in a graphic form, which is necessary for its fullest perception and visual analysis.

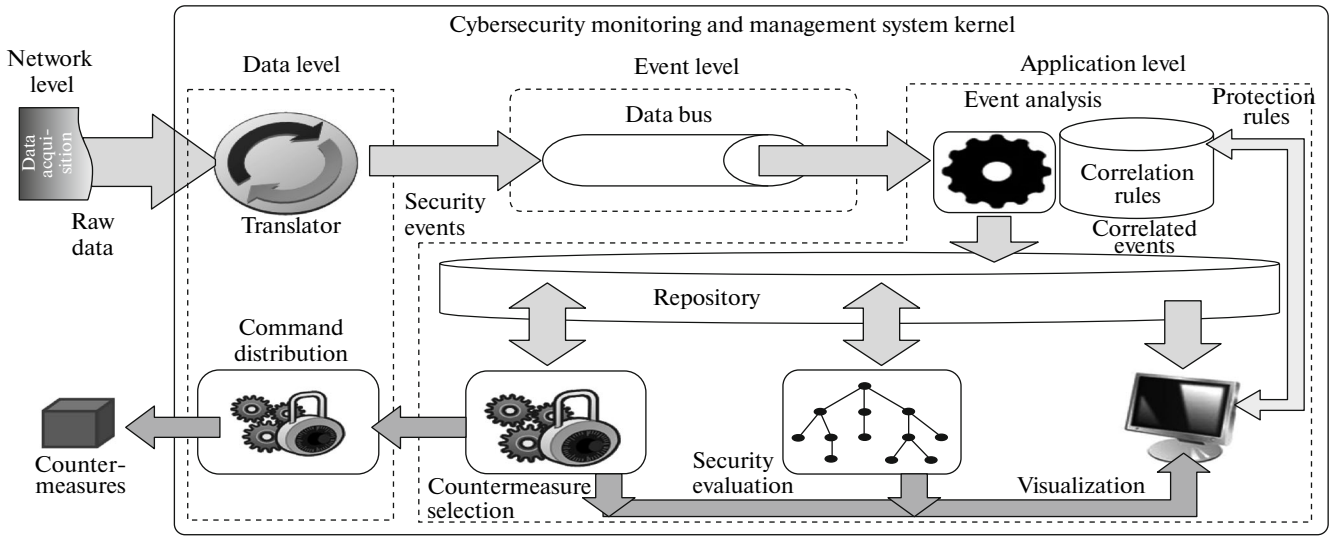

Fig. 1. Typical architecture of a new-generation cybersecurity monitoring and control system.

NEW-GENERATION CYBERSECURITY MONITORING AND MANAGEMENT SYSTEM COMPONENTS

The components mentioned in the previous section in their totality implement a higher level of functionality of the cybersecurity monitoring and management system developed within the MASSIF project; therefore, we may refer it to a new generation of such systems. Of greatest interest in this respect are several components that should be characterized in detail.

The first of them is the *translator*, which manages heterogeneous data and protects confidential information of remote infrastructural components by implementing interlevel data acquisition procedures, extended format processing, multilevel correlation, aggregation, event field coding, and anonymization.

The second extremely important component is the *data bus*. It creates a communication subsystem that ensures highly stable data exchange under computer attacks and other negative factors. Efficiency is achieved by a number of methods that employ the excessive accessibility in a physical network and enable real-time search for optimal routes of security-event data delivery. In order to restore missing packets, procedures are used to improve authenticity and minimize packet resend, thus minimizing time delays.

The *event analysis component* makes it possible to process several hundred thousand events per second without any corrections to the rules of event management. The constant storage of selected events in memory enables on-the-fly criminalistic analysis. Events may be processed in a distributed environment, in which high component scalability ensures a sufficiently high efficiency of event filtration, conversion, aggregation, abstraction, and correlation. The event analysis component has computational adaptability; i.e., it can control input loads. If an input load sharply increases, it automatically initiates task execution on new nodes, lifting off peak loads and distributing tasks evenly, and, in the case of downtime, it signs off unnecessary nodes.

We cannot but single out the *countermeasure selection component*, which, employing configuration rules, helps to develop and implement security policies for external systems in a coordinated manner. This component performs several functions: it determines policies on the basis of the model used for data access differentiation, manages conflicts, models policies, and consolidates security specifications through various infrastructural components. A response to a warning is carried out by analyzing and selecting possible countermeasures and is accompanied by the assessment of the value indicators of protection. If the optimal countermeasure is selected, the component creates new security policies aimed at security implementation. In the case of multiple cyberattacks, procedures to restore the protection level are considered.

The four above-described components were developed by foreign participants in the MASSIF project. The Russian participants in the project, represented by the team of the Laboratory of Computer Security Problems, SPII RAS, were responsible for the development of a hybrid ontological data repository, a component of attack modeling and security evaluation, and a visualization component.

The basis of the *data repository*, designed for the cross-platform integration of various components of the cybersecurity monitoring and management system [5–7], is a service-oriented architecture that implements the concept of building distributed information systems, in which program modules are united by

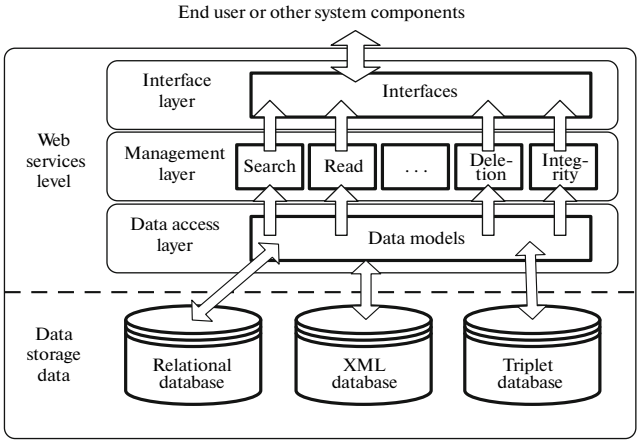

Fig. 2. Architecture of a security event repository.

well-defined interfaces and interaction rules. The architecture of the data repository, which complies with this approach, is divided into two levels; data storage and web services (Fig. 2).

The data storage level includes a relational database, an extensible markup language (XML) database, and a triplet database. The need to have three different databases in the repository is predetermined by the high efficiency of the hybrid ontological approach to the storage of security-event data, which combines the advantages of all basic models of data representation and ensures logical input and, consequently, decision making.

The relational database is a traditional tool for security-event information storage. It is ubiquitous in information security monitoring and management systems of the first generation. The next two types of databases are considered new trends in the development of data storage systems. The need for the XML database is predetermined by the fact that the XML language currently serves as the basic and, in some cases, standardized linguistic tool to represent information about various events. The triplet database is a tool to represent security knowledge and to implement logical inference. In addition, a triplet is understood as a semantic structure of a subject–predicate–object type. Triplets make it possible to formalize knowledge as ontologies. Ontologies, employing the capabilities and advantages of descriptive logic, which underlies them, make it possible to implement logical inference in cybersecurity monitoring and management systems, thus endowing them with intelligent capabilities for decision making.

The web-service implementation level is divided into a data access layer, a management layer, and an interface layer. The data access layer is a mediator between databases and various web services. On this layer, data are retrieved on request in line with the data models. Moreover, here the information access rules are verified. The management layer is responsible for data manipulation (search, read, delete, etc.) and data integrity; the interface layer is responsible for the interaction between the repository and the end user or other system components.

The *security evaluation component* is designed to analyze security events in order to detect attacks, recognize the behavior models of potential malefactors, and anticipate their subsequent steps. It can generate attack graphs and assess net protection by analyzing and calculating protection metrics. The obtained results are reflected in reports, which contain recommendations to improve the security level [7–14].

The input data of the security evaluation component include

- the parameters of the information infrastructure configuration;
- a set of authorities or access rules, which constitute the content of security policies;
- warnings and alerts formed in other system components;
- vulnerability data, attack templates, etc., which the component loads into the data repository from external information sources;
- the profiles of potential malefactors, including a large number of characteristics; and
- the required values of security metrics, which form the security requirements applicable to a cybersecurity monitoring and management system in general.

The output data obtained during the operation of the security evaluation component reflect

- vulnerabilities detected in the information infrastructure;
- possible cyberattack routes and targets (attack graphs);
- dependences between the information infrastructure's services that affect its security;
- the infrastructure's security "bottlenecks";
- corrected attack graphs in the case of network reconfiguration;
- predicted malefactor's further steps, which may occur in the current situation;
- the calculated values of security metrics used to assess the general level of infrastructure and its component protection;
- the possible consequences of attacks and countermeasures implemented; and
- proposals to improve the general level of protection, based on metrics, policies, and security instruments.

Let us characterize the elements of the security evaluation component, the architecture of which is

shown in Fig. 3. The loader fills the data repository with information received from external databases about vulnerabilities, attacks, configurations, platforms, and countermeasures. The generator of specifications converts information about network events, configurations, and security policies, obtained from the event analysis component or the user, into the internal representation. The malefactor-modeling module determines the individual characteristics of malefactors; the level of their qualification; the initial position (inside or outside the infrastructure, the possible access point, etc.); multiple authorities; already existing actions (attacks), the repetition of which can be predicted on the basis of data about certain events and warnings; and knowledge about the analyzed infrastructure.

The attack graph generator plots the graphs by modeling the sequences of the malefactor's attack actions in the analyzed infrastructure and using information about various possible cyberattacks, service dependences, network configurations, and security policies used. This element can also plot attack routes, taking into account the "zero day" vulnerabilities, the zero day being construed as unknown vulnerabilities used by malefactors to discredit the system resources.

The security analyzer supports the decision selection process by defining verification events and warnings, possible future security events, and countermeasures. Here probabilistic simulations of multistep attacks are generated; the efficiency of various countermeasures is calculated; and complex objects—individual attack sequences—are generated, as well as their totalities of the general attack graph. The security metrics of these objects are determined, supplementing the assessment of the general protection level, and, if necessary, recommendations to restore the general protection level are generated.

The final data about detected vulnerabilities, implemented and potential attacks, their strategies, and recommendations to improve the protection level, taking into account the set of countermeasures and formulating the content of various security policies, are formed by the report generator.

Another component created by the Russian participants in the MASSIF project is the *visualization component*, designed to analyze security information [15, 16]. The architecture of this component includes three layers: a user interface, control services, and graphic elements (Fig. 4). The first layer supports various graphic interfaces, beginning with a simple command line and ending with a complex multiwindow interface with control panels.

The layer of control services is seen as a visualization control module. Taking into account the function performed, this layer has two main elements: a controller of graphic elements and a service manager. The controller of graphic elements provides a standard

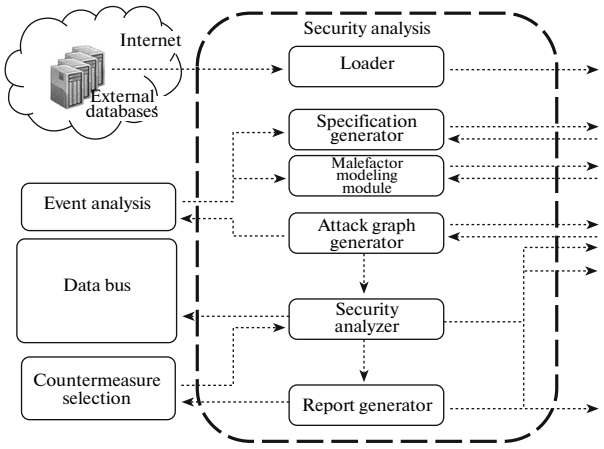

Fig. 3. Architecture of a security evaluation component.

interface for work with visualization flows, ensuring the creation and cessation of a graphic flow at the level of graphic elements. The service manager ensures the linkup of security monitoring and management services.

The layer of graphic elements includes a library of the necessary graphic primitives: graphs, radar charts, histograms, tree maps, geographical maps, etc. The graphic elements process input data, reflect them, and contribute to their interaction with the user.

APPLICATION SCENARIOS FOR NEW-GENERATION CYBERSECURITY MONITORING AND MANAGEMENT SYSTEMS

The above-considered characteristics of the construction and functioning of the components of new-generation cybersecurity monitoring and management systems make it possible to formulate proposals how to use these systems. The main advantage of the developments within the MASSIF project lies in the significant extension of the field of their application compared to traditional commercial systems of this type. The latter, as was already mentioned, are oriented primarily at their use in small and medium-sized computer networks with a low degree of territorial distribution, small or medium-sized productivity (up to several thousand events processed per second), and a high reliability and authenticity of data exchange. New-generation systems, on the contrary, are able to operate in information infrastructures with a high degree of territorial distribution due to the use of the Internet as a communication subsystem, a high level of productivity (up to several hundred thousand events processed per second), low reliability, and a low authenticity of data exchange.

Three scenarios were selected and analyzed as test fields of application to demonstrate the advantages of

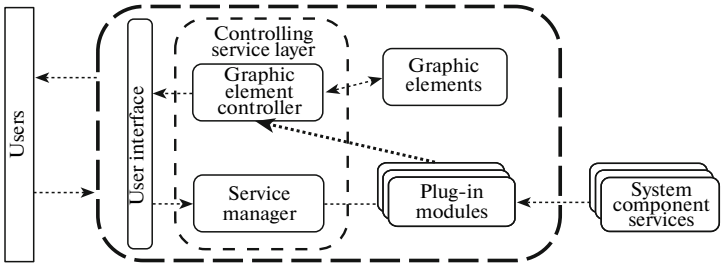

Fig. 4. Visualization component architecture.

the new-generation cybersecurity monitoring and management systems.

The *first scenario* considered a computer infrastructure that corresponded to the infrastructure of the Olympic Games. It is characterized by the need to process several hundred thousand events per second and, consequently, a high productivity. Three types of servers were the objects of unauthorized access on the part of malefactors: the accreditation server, the event server, and the authentication server, the first two servers being parts of the network's demilitarized zone. These servers are used to register athletes and referees, as well as sporting event data. The authentication server belongs to the central part of the protected infrastructure. All servers process information of different types, coming both from workstations that are elements of the local computer net infrastructure of the Olympic Games and from the outside via the Internet. The malefactor who planned to attack the above servers was an external user in this scenario.

A typical attack scheme includes five stages. At the first stage, remote control is established over the sporting event server in order to ensure its further analysis. During this stage, vulnerabilities are scanned, malicious software is embedded, the code is remotely executed, and the files on this server are cracked. At the second stage, the malefactor increases his authorities by "brute force" attacks on the password of the local administrative account of the operating system (this attack is based on password guessing). At the third stage, the computer network is investigated for available vulnerabilities in order to identify open ports on the authentication server; at the fourth stage, the "zero day" attack is carried out aimed at a previously unknown vulnerability. Thanks to the execution of this attack, the malefactor acquires the possibility to execute remotely ad hoc commands on the authentication server. Finally, the fifth stage consists in finding an account that ensures access to the accreditation server's applications.

The malefactor's actions are reflected in the unusual activity of the servers of authentication and accreditation. Despite the fact that the activity growth is accessible for observation, its opportune identification against the backdrop of a great amount of other security events processed by the system becomes a hard task with which the new-generation cybersecurity monitoring and management systems are designed to cope. This is the specifics of their functioning.

The model of the *second scenario* of the possible implementation of the new-generation cybersecurity monitoring and management systems is shown in Fig. 5a. The protection object in this case is a territorially distributed computer infrastructure in which security-event data acquisition and delivery from the periphery to the center and the transmission of decisions on the use of countermeasures from the center to the periphery are carried out via a telecommunication medium exposed to multiple impacts. The infrastructure under consideration includes remote elements, which are mobile devices; a confidentiality-providing system; a system of communications (i.e., data packets delivery) and a data storage system, each of high stability; and a system of centralized event correlation. According to the scenario, the malefactor attempts an attack from a remote mobile device, and the cybersecurity monitoring and management system is to support a high reliability of data transfer between the elements of the distributed infrastructure and to correlate events under the possible incompleteness and inconsistency of the data stored.

The *third scenario* considers a critical information infrastructure designed to manage waterworks (a dam) (Fig. 5b). Its characteristic feature is the need to ensure the joint data processing of security events coming both from traditional sources and from various sensors, which record the physical parameters of the state of the elements of the waterworks infrastructure (in the modeled case, the water surface level, pressure, temperature, etc.).

The cybersecurity monitoring and management systems together with the dam control system comprise the control center. The control system includes the chief control server (in the figure, CCS) and a database, containing the values of physical parameters. The parameter values are collected via remote control servers (RCSs). Overall, these elements execute operating services to control the dam. The cyber-

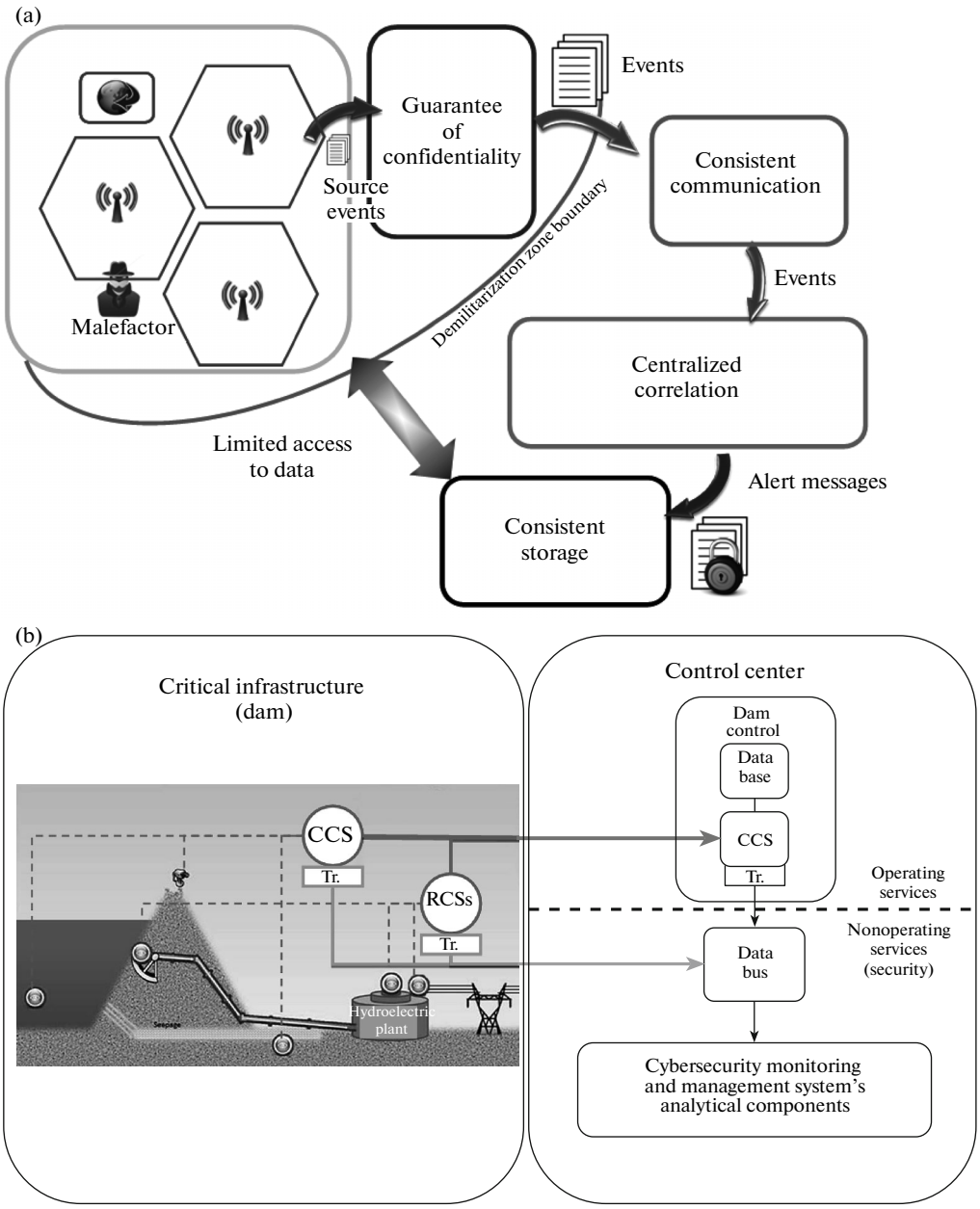

Fig. 5. Information infrastructure protection with a new-generation cybersecurity monitoring and management system. (a) For a distributed infrastructure and (b) for a critical infrastructure.

security monitoring and management system includes special event translation agents (Tr.) on all control servers and supplements the capabilities of the system of data control of nonoperating security services. The values of parameters recorded by the physical sensors are transmitted via the data bus to the system's analytical components, and information from the database of the dam control system also comes there. As a result, the cybersecurity monitoring and management system implements its main task in this scenario: it improves the security level of the critical infrastructure by implementing the interlevel correlation of security events at the level of computer-network elements and at the level of physical sensors.

* * *

The development of methods and models in the sphere of security event data representation, collection, storage, and processing, which make it possible to comply with the current requirements for the cybersecurity monitoring and management system, is an urgent scientific problem of great national and eco-

nomic significance, setting new directions for scientific research in the sphere of information security.

The solutions considered in this article can be used either as new-type cybersecurity monitoring and management systems or independently to improve the efficiency of the existing protection tools and systems in order to achieve a higher level of security of information infrastructures in various subject areas.

ACKNOWLEDGMENTS

This work was supported by the Russian Foundation for Basic Research (projects nos. 13-01-00843-a, 13-07-13159-ofi_m_RZhD, 14-07-00697-a, and 14-07-00417-a), the basic research program of the RAS Department of Nanotechologies and Information Technologies (project no. 2.2), the ENGENSEC project of the EU TEMPUS program, and government contracts nos. 14.604.21.0033, 14.604.21.0137, 14.604.21.0147, and 14.616.21.0028.

REFERENCES

1. MASSIF FP7 Project. Management of Security Information and Events in Service Infrastructures. http://massif-project.eu
2. I. V. Kotenko and I. B. Saenko, "SIEM systems for security information and events management," Zashchita Informatsii. Insaid, No. 5 (2012).
3. I. V. Kotenko, I. B. Saenko, O. V. Polubelova, and A. A. Chechulin, "Security information and event management technologies for computer network protection," Probl. Inf. Bezopasnosti. Komp'yut. Sist., No. 2 (2012).
4. I. V. Kotenko, V. V. Vorontsov, A. A. Chechulin, and A. V. Ulanov, "Proactive mechanisms of network worm protection: Approach, implementation, and experimental results," Inf. Tekhnol., No. 1 (2009).
5. I. Kotenko, O. Polubelova, and I. Saenko, "Data repository for security information and event management in service infrastructures," in *SECRYPT 2012—Proceedings of the International Conference on Security and Cryptography, Rome, Italy, July 24–27, 2012* (SciTePress, 2012), pp. 308–313.
6. O. V. Polubelova, I. V. Kotenko, I. B. Saenko, and A. A. Chechulin, "Ontologies and logical inference for security information and event management," Sist. Vysokoi Dostupnosti, No. 2 (2012).
7. I. Kotenko, O. Polubelova, and I. Saenko, "The ontological approach to SIEM data repository implementation," in *2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical, and Social Computing. GreenCom 2012* (IEEE Computer Society, Los Alamitos, California, 2012), pp. 761–766.
8. I. V. Kotenko, I. B. Saenko, O. V. Polubelova, and A. A. Chechulin, "Security information and event management technology for information protection in critical infrastructures," in *Proceedings of SPII RAS* (Nauka, St. Petersburg, 2012), No. 1 [in Russian].
9. I. V. Kotenko, M. V. Stepashkin, D. I. Kotenko, and E. V. Doinikova, "Assessment of information system security based on plotting the trees of socioengineering attacks," Izv. Vyssh. Uchebn. Zaved., Instrument Making, No. 12 (2011).
10. I. Kotenko, A. Chechulin, and E. Novikova, "Attack modelling and security evaluation for security information and event management," in *SECRYPT 2012—Proceedings of the International Conference on Security and Cryptography, Rome, Italy, July 24–27, 2012* (SciTePress, 2012), pp. 391–394.
11. I. Kotenko and A. Chechulin, "Common framework for attack modeling and security evaluation in SIEM systems," in *2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical, and Social Computing. GreenCom 2012* (IEEE Computer Society, Los Alamitos, California, 2012), pp. 94–101.
12. I. Kotenko and M. Stepashkin, "Network security evaluation based on the simulation of malefactor's behavior," in *SECRYPT 2006—Proceedings of International Conference on Security and Cryptography, Setúbal, Portugal, August 7–10, 2006* (INSTICC, 2006), pp. 339–344.
13. I. V. Kotenko, M. V. Stepashkin, and V. S. Bogdanov, "Architectures and models of active security analysis components based on the simulation of malefactor actions," Probl. Inf. Bezopasnosti. Komp'yut. Sist., No. 2 (2006).
14. J. F. Ruiz, R. Harjani, A. Mana, V. Desnitsky, I. Kotenko, and A. Chechulin, "A methodology for the analysis and modeling of security threats and attacks for systems of embedded components," in *Proceedings of 20th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2012* (Garching, 2012), pp. 261–268.
15. E. S. Novikova and I. V. Kotenko, "Visualization mechanisms in SIEM systems," Sist. Vysokoi Dostupnosti, No. 2 (2012).
16. E. S. Novikova and I. V. Kotenko, "Visualization technologies for security information and event management," in *Proceedings of SPII RAS* (Nauka, St. Petersburg, 2012), No. 4 [in Russian].

Translated by B. Alekseev