DOI: https://doi.org/10.17721/ISTS.2019.1.36-41
UDC 681.3.06

MODELING OF INFORMATION SECURITY SYSTEM IN COMPUTER NETWORK

Bogdan Korniyenko [1]
orcid.org/0000-0002-2521-0878

Liliya P. Galata [2]
orcid.org/0000-0002-7978-3954

[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine, bogdanko@i.ua
[2] National Aviation University", Kyiv, Ukraine, galataliliya@gmail.com

Paper history:
Received 17.06.2017
Accepted 25.07.2017

Keywords:
model;
modeling;
simulation;
security;
threats.

Abstract: *This article presents simulation modeling process as the way to study the behavior of the Information Security system. Graphical Network Simulator is used for modeling such system and Kali Linux is used for penetration testing and security audit. To implement the project GNS3 package is selected. GNS3 is a graphical network emulator that allows you to simulate a virtual network of more than 20 different manufacturers on a local computer, connect a virtual network to a real one, add a full computer to the network, Third-party Applications for network packet analysis are supported. Depending on the hardware platform on which GNS3 will be used, it is possible to build complex projects consisting of routers Cisco, Cisco ASA, Juniper, as well as servers running network operating systems. Using modeling in the design of computing systems, you can: estimate the bandwidth of the network and its components; identify vulnerability in the structure of computing system; compare different organizations of a computing system; make a perspective development forecast for computer system; predict future requirements for network bandwidth; estimate the performance and the required number of servers in the network; compare various options for computing system upgrading; estimate the impact of software upgrades, workstations or servers power, network protocols changes on the computing system. Research computing system parameters with different characteristics of the individual components allows us to select the network and computing equipment, taking into account its performance, quality of service, reliability and cost. As the cost of a single port in active network equipment can vary depends on the manufacturer's equipment, technology used, reliability, manageability. The modeling can minimize the cost of equipment for the computing system. The modeling becomes effective when the number of workstations is 50-100, and when it more than 300, the total savings could reach 30-40% of project cost.*

Анотація: *У статті розглянуто процес імітаційного моделювання, як спосіб дослідження поведінки системи інформаційної безпеки. Для моделювання такої системи використовується Graphical Network Simulator, а для тестування проникнення та аудиту безпеки використовується Kali Linux. Для реалізації проекту обрано пакет GNS3. GNS3 – це графічний емулятор мережі, який дозволяє моделювати віртуальну мережу з мережевого обладнання більше ніж 20 різних виробників на локальному комп'ютері, приєднувати віртуальну мережу до реальної, додавати в мережу повноцінний комп'ютер, підтримується сторонні програми для аналізу мережевих пакетів. Залежно від апаратної платформи, на якій буде використовуватися GNS3, можлива побудова комплексних проектів, що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, а також серверів під управлінням мережевих операційних систем. Використовуючи моделювання при проектуванні обчислювальних систем, можна: оцінити пропускну здатність мережі та її складових; виявити вразливості в структурі обчислювальної системи; порівнювати різні варіанти проектування обчислювальної системи; скласти перспективний план розробки комп'ютерної системи; прогнозувати вимоги до пропускної здатності мережі; оцінювати продуктивність і необхідну кількість серверів у мережі; порівняти різні варіанти модернізації обчислювальної системи; оцінити вплив оновлення програмного забезпечення, робочих станцій, серверів, зміни мережних протоколів на обчислювальну систему. Дослідження параметрів обчислювальної системи*

з різними характеристиками окремих компонентів дозволяє вибрати мережу і обчислювальну техніку, враховуючи її продуктивність, якість обслуговування, надійність і вартість. Оскільки вартість одного порту в активному мережному обладнанні може змінюватися в залежності від виробника, використовуваної технології, надійності, керованості. Моделювання може мінімізувати вартість обладнання для обчислювальної системи. Моделювання стає ефективним, коли кількість робочих станцій становить 50-100, а при більш ніж 300 - загальна економія може досягати 30-40% від вартості проекту.

1. INTRODUCTION

Efficient construction and usage of corporate information systems has become an extremely important task, especially in insufficient funding of information technology in enterprises. Evaluation criteria for efficiency are the cost reducing of the information system implementation, current and nearest future requirements compliance, the opportunity and the cost of further development and transition to new technologies.

The information system core is a computing system that includes next components: cable network and active network equipment, computer and peripheral equipment, data storages (libraries), system software (operating systems, database management systems), special software (monitoring and network management) and in some cases the applied software.

Two main types of computer network modeling can be considered: analytical and simulation modeling [1].

Analytical models of networks are built on the basis of mathematical tools of queuing theories, probability and Markov processes, as well as methods of diffuse approximation [1]. Also, as methods of analytical network modeling, differential and algebraic equations can be used that describe the network behavior in time.

When using analytical modeling, it is often possible to obtain models for solving a fairly wide range of computer network research tasks. At the same time, analytical network models have a number of significant drawbacks, which include:

- significant simplifications inherent in most analytical models (such simplifications sometimes call into question the results of analytical modeling);
- cumbersome calculations for complex models.

Thus, despite the significant achievements of analytical modeling, many real-life situations cannot be adequately represented using appropriate mathematical models. In some cases, this is hampered by a certain "rigidity" of mathematics as a language for describing and representing events and phenomena. In other cases, even if it is possible to formalize the life situation under consideration through the construction of a mathematical model, the optimization problem obtained on its basis may be too complicated for modern algorithms for solving problems of this class [1].

The second type of computer network modeling is simulation modeling. This type of simulation is often the best, and sometimes the only way to study real systems, including networks.

The term "simulation modeling" means that the processes under study are difficult to predict, and to predict the behavior of a system, a computational experiment (imitation) is required with given initial data.

The difference between the analytical and simulation models is that in the latter, instead of an explicit mathematical description of the relationship between the input and output variables, the real system is divided into a number of fairly small (in functional terms) elements or modules [1]. Then, the behavior of the source system is simulated as the behavior of a set of these elements, which are connected in a certain way (by establishing the corresponding relationships between them) into a single whole. The computational implementation of such a model begins with the input element, then goes through all the elements until the output element of the model is reached.

2. MODELING

Now the most common approach in information systems design is to use expert estimates. According to this approach, experts in the field of computing tools, active network equipment, cable networks, design computing system to solve the specific task or class of tasks, based on their experience and expert estimates. This approach minimizes the cost of the design stage, quickly estimate the cost of implementing the information system. However, decisions obtained by using expert estimates are subjective, hardware and software requirements as the assessment of guarantees for efficiency of proposed system project are subjective too.

As an alternative may be used approach, which involves the development of models and modeling (simulation work - simulation) of computing system behavior. The modeling is a fundamental method for studying the behavior of complex systems [2-5].

The modeling is one of the main methods of knowledge, and a form of reflection of reality. The

modeling is to clarify or reproduction of certain properties of real objects, things and events through other objects, processes, events, or through abstract descriptions such as image, plan, map, set of equations, algorithms and applications.

The model is defined as "a system that is provided or material implemented, that is replaced the real object (system) in the process of cognition or analyzing, while retaining some of the most important features for its research, and its study gives us new information about the object.

Here are the main types of models used in practice to describe the different processes and systems:

- the conceptual model – the model describes the system using special characters, symbols, operations or using natural or artificial languages;
- the physical model - the system reproduces based on the ratio of similarity, that is resulting from the similarity of physical phenomena;
- the structural and functional model - as a model uses scheme (block diagram), tables, graphs, diagrams and drawings with special rules of their union and transformation;
- the math model is a math representation of reality, the description of some phenomenon or system using math concepts and symbols;
- the simulation model - economic and math model uses in the experimental study of system or phenomena by using personal computers.

These types of models can be used both individually and a few at a time, also, when you use simulation modeling, it involves all of these types or their separate techniques. The simulation model allows us to visualize the final or intermediate result dynamically, that is an important aspect for a successful understanding the received results by persons who did not participate in its development.

3. SIMULATION MODEL

Common definitions of term “simulation modeling”:

- it is the method allows to build models that describe the processes as they would take place in reality. Such model can be "played" for a single test or set of tests. The results will be determined by the random behavior of the process;
- it is the research method in which studied system is replaced by a model that accuracy describes the real system, with which experiments are conducted to obtain information about this system;
- it is the special case of math modeling. There is a class of objects, for which have not developed analytical models or solution methods of resulting model for various reasons. In this case, the analytical model is by the simulator or simulation model;
- it is logical and mathematical description of an object that can be used to experiment on your computer in order to design, analysis and assessment of the object.

Simulation modeling is used to study the behavior of the system by using math tools and computing equipment. The calculation of the required results may be automated by using computing technology, with only initial data, for example, been obtained statistically. It is especially important, when complex system that consist of many components is being used, because for calculation of required results you need to use cumbersome formulas usually. Simulation modeling is applied to study the behavior of various systems, including the information one [6-8].

Mainly in information systems modeling there is an aim to achieve information about request processing time or resource load level. As for computing networks, their simulation models reproduce the processes of message generation by applications, of splitting messages into specific protocols packets and frames, of delays in processing messages, packets and frames within the operating system, of computer access to the shared network environment, of router incoming packets processing and etc. No need to buy expensive equipment by using simulation modeling network - its work simulates by programs that accurately reproduce such equipment main features and options.

4. SIMULATION ENVIRONMENT

It was offered to use simulation modeling for determination the actual security threats [9-12]. GNS3 Cisco Systems software have been selected as the simulation environment (Fig 1).

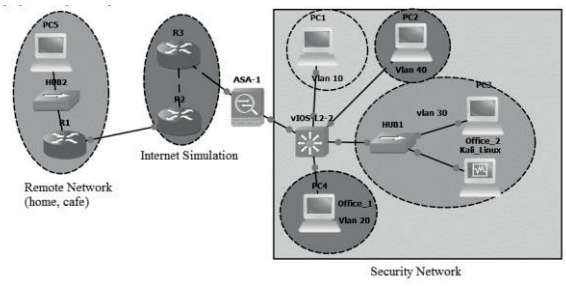

Fig.1 - The simulation model of information security system in computer network

The choice of this software due to the following factors:

- a process of creating models is facilitated by using a graphical development environment;

- previously created modules and libraries can be used to create new models;
- object-oriented approach to model building;
- a large number of built-in libraries for creating simulation models;
- models can be run at any software and hardware platform;
- a simulation model can be run without development tools.

Graphical Network Simulator GNS3 is a cross-platform program with open source. It is based on popular Dynamips (CISCO IOS emulator), Dynagen (Dynamips text interface) and Pemu (Cisco PIX emulator).

GNS3 provides easy to use GUI, and a range of other features. You can model the new configuration, various images of IOS, or perhaps, make fully reconstruction of some complex network parts. That is much easier with this program than its be in a real network. The product processes the installation and configuration of essential utilities automatically. The GNS3 installation package includes all emulators. In the case of GNS3 installation on the Microsoft Windows operating system, you must also install WireShark, it is necessary to intercept monitor network packets and libraries.

Sometimes, it is not enough network devices in the company and there is no router, which deals with internal networks routing, but there is only L2-switch and security device Cisco ASA with IOS 8.4.2 version. So, it is necessary to set additional functionality on Cisco ASA, such as routing. Similarly, we have only one interface to connect with the L2-switch. Also, we need to configure remote users' connections by VPN.

There is the next task: the networking between internal networks should be organize to meet the requirements of security. The guest network access should be organized only to "INTERNET" with limited speed of 1024 Kb. The remote users connect should be organize through Remote Access VPN, therefore remote users should connect to the internet via Cisco ASA device and have access to the internal resources of the company. Internal website should be available on "INTERNET". All of this task should be done through CLI. We have a central office with installed Cisco ASA device and L2-switch. Four networks (VLANs) have been created at switch, which submitted to security device through Trunk.

There are the characteristics of each VLAN-s:

- Vlan_Office_1 - network 192.168.2.0/24.

Security Level is 100. It is uses for first part of employees. There are the Internet access from this subnet, and Vlan_Office_2, Vlan_DMZ and Vlan_Guests access;

- Vlan_Office_2 - network 192.168.3.0/24.

Security Level is 100. It is uses for second part of employees. There are the Internet access from this subnet, and Vlan_Office_1, Vlan_DMZ and Vlan_Guests access;

- Vlan_DMZ - network 192.168.1.0/24.

Security Level is 50. There is a Web-Server (WWW-SRV) with company's website in this network. Accordingly, it is available from Internet at port 80 (TCP) and there are access from Vlan_Office_1, Vlan_Office_2 subnets to this network and from Vlan_Guests subnet at 80th port;

- Vlan_Guests - Guest subnet 192.168.4.0/24.

It is uses for "guests" who came to our office. Security Level is 10. There are the Internet access from this subnet with limit speed of 512 Kb and access to the internal website (SRV-WWW) only at 80th port.

There is a network, that simulates "INTERNET", which uses two routers (Router_1 and Router_2). There is loopback-interface (IP-address 1.1.1.1) at Router_1, which will be use to check for the "INTERNET". Dynamic routing protocol OSPF is used for routes exchange. Also, there is a remote user, which is placed in the subnet 192.168.5.0/24 (say it is internet-cafe) behind Remote_Router. This remote user has access to the Internet but he is considered dangerous without VPN connection to the central office.

A simulation model consists of protected and unprotected networks. The main element of information security system is the firewall ASA 8.4, a platform for attack- set Kali Linux. Kali Linux is modern Linux-distribution for penetration testing and security audit. Kali is a complete reassembly BackTrack Linux, fully according to Debian development standards.

All new infrastructure has been revised, all the tools were analyzed and packaged, and we switched to Git for our VCS.

- There are more than 300 tools for penetration testing: After considering each tool that was included in BackTrack, we have removed a large number of tools that either do not work or duplicate other tools with similar functionality.
- Kali Linux is completely free and always will be free. You will never have to pay for Kali Linux.
- Git tree with open source code: our tree is open to all, and all of sources available for set up or rebuild packages.
- FHS compliant: Kali was designed to observe the Filesystem Hierarchy Standard, which allows all Linux users easily find executable files, support files, libraries, etc.
- Wide support for wireless devices: Kali Linux was built to support many wireless devices, allowing

it to work correctly with a wide range of hardware devices and making it compatible with many USB and other wireless devices.

- Special core patches from injection: developers often need to audit wireless networks, so our core includes the latest patches for them.
- Secure Development Environment: Kali Linux development team consists of a small group of trusted persons who can add packages or interact with storage only by using several secure protocols.
- GPG signed packages and repositories: All packages are signed by each individual Kali developer when they are created and recorded, and then the repository signed packages also.
- Multilingual: Kali has a true multi-language support, allowing most users to work in their native language and to find the tools needed for the job.
- Customizable: You can as easy as possible customize Kali Linux to your taste, down to the core.
- Support ARMEL and ARMHF: Kali supports ARM-systems and has installations for ARMEL and ARMHF systems. Kali Linux ARM repository is integrated with the main distribution.

LOIC was used to implement attacks. The program performs a distributed attack such as "denial of service" by TCP-, UDP-packets or HTTP-requests regular transfer to the certain site or host with a goal to destroy the target node. There is also an edition of the program LOIC Hive Mind, that automatically receive the task to attack via IRC, RSS or Twitter, which allows centralized DDoS-attacks.

Attacks occur from a remote location to internal subnet (Office_1, Office_2, DMZ, Guests) with different security levels. There are customized security levels: offices - security level is 100, the traffic between offices is not filtered. DMZ security level – 50, Guests -10. Offices trafik is unrestricted with other subnets, there is access from DMZ to Guest subnet, there is access from the guest subnet only to the Internet. Internetworking is emulated by two routers with loopback-interface.

5. CONCLUSIONS

Using modeling in the design of computing systems, you can:

- estimate the bandwidth of the network and its components;
- identify vulnerability in the structure of computing system;
- compare different organizations of a computing system;
- make a perspective development forecast for computer system;
- predict future requirements for network bandwidth;
- estimate the performance and the required number of servers in the network;
- compare various options for computing system upgrading;
- estimate the impact of software upgrades, workstations or servers' power, network protocols changes on the computing system.

Research computing system parameters with different characteristics of the individual components allows us to select the network and computing equipment, taking into account its performance, quality of service, reliability and cost. As the cost of a single port in active network equipment can vary depends on the manufacturer's equipment, technology used, reliability, manageability.

The modeling can minimize the cost of equipment for the computing system. The modeling becomes effective when the number of workstations is 50-100, and when it more than 300, the total savings could reach 30-40% of project cost.

6. REFERENCES

[1] Klaus Wehrle, James Gross. *Modeling and Tools for Network Simulation*. Hardcover, 2010, 256 p.

[2] Korniyenko, B., Yudin, O. Galata, L. Research of the Simulation Polygon for the Protection of Critical Information Resources. *CEUR Workshop Proceedings, Information Technologies and Security, Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017)*, Kyiv, Ukraine, November 30, 2017, Vol-2067, 2017, pp.23-31.

[3] Korniyenko, B. Model of Open Systems Interconnection terms of information security. *Science intensive technology*, № 3 (15), 2012, pp. 83 – 89.

[4] Korniyenko, B., Yudin, O., Novizki,j E. Open systems interconnection model investigation from the viewpoint of information security. *The Advanced Science Journal*, issue 8, 2013, pp. 53 – 56.

[5] Korniyenko, B., Yudin, O. Implementation of information security a model of open systems interconnection. *Abstracts of the VI International Scientific Conference "Computer systems and network technologies»* (CSNT-2013), 2013, p. 73.

[6] Korniyenko, B. *Information security and computer network technologies*: *monograph*. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland, 2016, 102 p.

[7] Korniyenko, B., Galata, L., Kozuberda, O. Modeling of security and risk assessment in information and communication system. *Sciences of Europe*, V. 2., No 2 (2), 2016, pp. 61 -63.
[8] Korniyenko, B. The classification of information technologies and control systems. *International scientific journal*, № 2, 2016, pp. 78 - 81.
[9] Korniyenko, B., Yudin, O. Galata, L. Risk estimation of information system. *Wschodnioeuropejskie Czasopismo Naukowe*, № 5, 2016, pp. 35 - 40.
[10] Korniyenko, B., Galata, L., Udowenko, B. Simulation of information security of computer networks. *Intellectual decision-making systems and computing intelligence problems (ISDMCI'2016): Collection of scientific papers of the international scientific conference*, Kherson, Ukraine, 2016, pp. 77 - 79.
[11] Korniyenko, B. *Cyber security - operating systems and protocols*. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland, 2017, 122 p.
[12] Korniyenko, B., Galata, L. Design and research of mathematical model for information security system in computer network. *Science intensive technology*, № 2 (34), 2017, pp. 114 - 118.

Korniyenko Bogdan Yaroslavovich,
Education and qualifications: Doctor of Technical Sciences, Associate Professor
Employment: National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Professor of the Department of Automation and Control in Technical Systems, since 2018.
Interests: information security, information technology
Science: Author of more than 160 scientific papers.

***Galata Liliya Pavlivna**,*
Education and qualifications:
- National Aviation University, engineer of computer systems, 2005;
- National Aviation University, the postgraduate study program for Doctors of Philosophy at the specialty 122 «Computer Science and Information Technologies», from 2017.
Employment: National Aviation University, assistant of the Department of computerized information security systems, since 2005.
Interests: information security, information technology, web development.
Science: author of more than 40 scientific publications.