Information & Security: An International Journal

Zhukovyts'kyy & Ostapec, vol.35, 2016, 81-97 https://doi.org/10.11610/isij.3504

DEVELOPMENT OF TOOLS FOR PRACTICAL RESEARCH ON CYBERSECURITY IN MSC THESES

Igor ZHUKOVYTS'KYY and Denis OSTAPEC

Abstract: The article analyses methods of creating and implementing practical courses on cybersecurity, including distance learning courses. It outlines a number of methodologies and corresponding hardware/firmware structures of the organization of such courses. Next, the authors consider the possibility of tying the courses in the standard program complexes of distance learning. It is proposed to use the interactive simulation models for practical skill training in the area of cybersecurity. For teaching the skills of server setting, the creation of client-server simulation models is proposed. The paper considers the proposed methodologies for development of such educational complexes in the master's theses of students of the specialty "Security of Information and Communication System" in Dnipropetrovsk National University of Railway Transport named after Academician V. Lazaryan, and provides a number of recent examples.

Keywords: Practical courses on cybersecurity, cybersecurity training methodology, interactive simulation models, client-server complexes, distance learning systems.

Introduction

The modern development of society is determined by the rapid increase in the rate of knowledge aging. Therefore, the need to update this knowledge increases. According to general statistics, nearly 50% of professional knowledge is acquired by the specialists after graduating. So they are often forced to improve their knowledge on-the-job. The latter is the front most for employees of large companies. This is a classic problem for the companies to let the employees for examination period, as well as for those who live in remote regions. Within the framework of the project Tempus SEREIN (Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains) it is developed the training programs, corresponding courses in the area of cyber security for both the students of different education levels (masters, Ph.D. students) and for post-graduate studies.

Published by ProCon Ltd., www.procon.bg, under Creative Commons 4.0 Attribution-NonCommercal-ShareAlike International license (CC BY-NC-SA 4.0).

Work Related Analysis

There is number of formation and implementation mechanisms of courses on cyber security. Full-time courses are offered in a number of well-known universities.[1–3] It proposed a number of part-time distant learning courses.[2,4,5] As a rule, the courses include a lecture and practical material. The lecture material located on educational sites is a text material with graphic illustrations. Practice offers a discussion, decision of some problem. Some courses provide independent program complexes, which make it possible to simulate the operation of equipment (for example, the Cisco PacketTracer complex [5] simulates the setup and operation of computer network with the Cisco equipment).

The use experience of competitions in the area of cyber security, organized by the Lincoln Laboratory of Massachusetts Institute of Technology [6] to increase the professional level of students is of some interest. In these competitions the participants are provided with the special area (laboratory) equipped by servers and clients. The contestants attack the servers from the client places. Servers are set either by professional staff of the Lincoln Laboratory, or the participants of the competition.

One of the forms of knowledge gaining is distant education, which is becoming widespread.

In the area of modern distant education the systems using web technologies became widespread. Among these the most common are:

- IBM Lotus Learning Management System [7];
- IBM Lotus Workplace Collaborative Learning [8];
- WebCT Campus Edition [9];
- Prometheus [10];
- Moodle.[11]

Such systems are omni-purpose and can be used for training in many areas, including the field of cyber security. These systems are aimed primarily at supplying the students with the lecture material in the traditional form (text with illustrations), and the testing of students according to the results of the lecture material studying.

Purpose and Structure of the Work

The purpose of the article is to discuss the experience of fulfilment and use of master's theses of students of the Dnipropetrovsk National University of Railway Transport in the area of development of the program complexes for interactive and distant practical research in the field of cyber security.

The article observes the proposed methodology of practical research implementation, the optional versions of hardware/firmware complexes used for this purpose. As we go forward we consider the specific examples of developments. The research results and their practical use are analysed at the end.

The Empirical Research Procedure

During development of the empirical research procedure, the following was considered.

The first task:

- detailed study of algorithms and protocols in the field of cryptography, steganography, security of networks and servers;
- the students should be provided with the illustrative material of the studied entity in the multimedia, animation format with the ability of step by step detailed examination of algorithm, protocol;
- the algorithmic interactive testing of the student (both the trial and the control one) should be possible: interrogation of each step of the algorithm, protocol; selection of the steps sequence; interactive fulfilment of the separate steps, etc.

The second task:

- the research of security methods in the network (correct server setting, counteracting the attacks on the server);
- students should be provided with the test area, where they can explore the mechanism of server settings and check the setting during the various attacks on the server.

For each task:

- students should be provided with a detailed reference material on the studied entity in the classic text format with illustrative material;
- it should be possible to test the student; the testing methods, both the traditional (interrogation) and the additional one (the interrogation for each step of the algorithm, protocol, the choice of the step sequence, the interactive fulfilment of the separate steps, etc.);
- the testing can be both the trial and the control one;
- personalized control testing results should be available to teacher, students cannot change the result of this test.

To implement the possibility of demonstration and study of functioning of the studied entity in multimedia and animation format it was decided to develop a number of simulation models.

To implement interactive fulfilment by the student of the separate steps of the algorithm, protocol the same simulation model set to test mode can be used. A separate simulation model for testing purposes can be also developed.

Since the Moodle system is taken in the university as the base one for the distant education, it is advisable to conduct the part of the functions of practical research (providing the reference and the lecture material in the traditional format, the traditional testing on the subject) in the framework of Moodle system, which is tied in the simulation models.

Implementation Variations of the Automated System of Practical Research

The practice of automated systems development for the practical research (laboratory works) implementation in the area of cyber security in the master`s theses in Dnipropetrovsk National University of Railway Transport have long been developing. In the beginning, it was autonomous program complexes that were run on each computer. The next step is the association of autonomous program complexes in the local area network of the laboratory, decollation of the student`s and teacher`s computers, the location of the database on the server.

Currently, the development of systems for distant performance of laboratory works that are tied in the Moodle system (the system taken by the University as the base for distant education) is the common practice in the University. The structure of such hardware/firmware complex is shown in the Figure 1.

The system of distant laboratory work performance includes the following main functional blocks:

- server’s computer;
- student’s computer;
- teacher’s computer;
- mail server.

The above mentioned components interact using the Internet protocol HTTP (Hypertext Transfer Protocol).

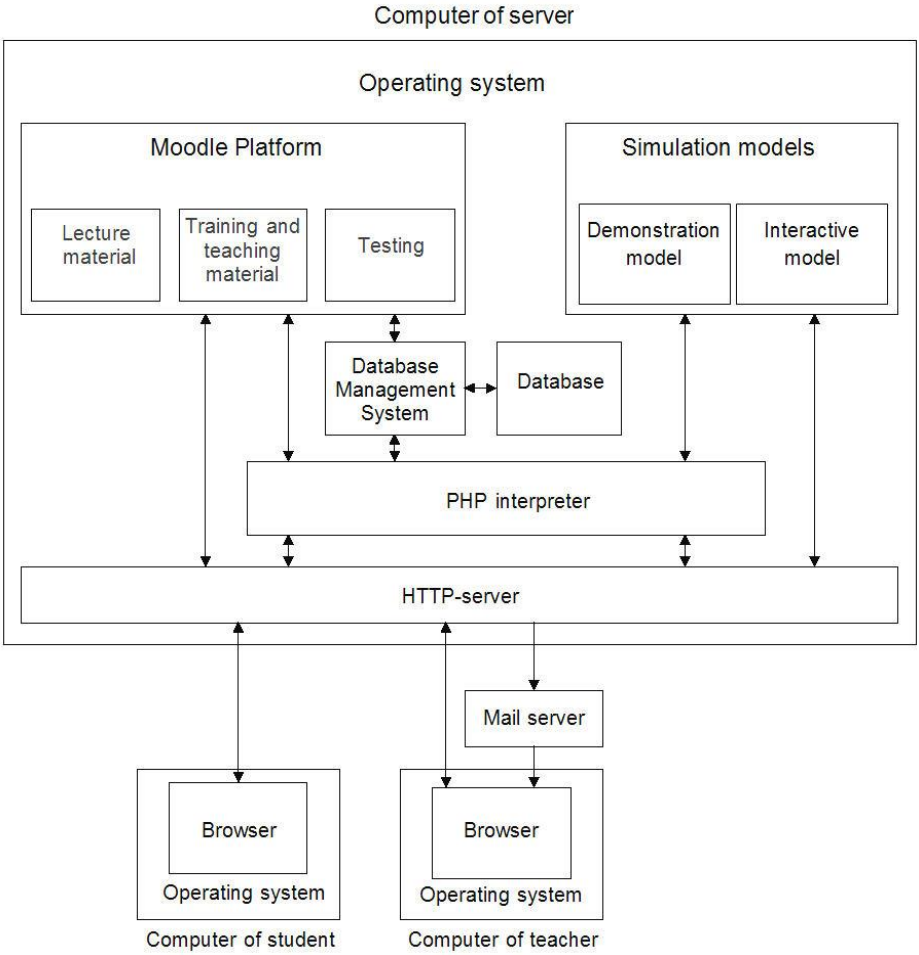

Figure 2: General structure of the system for distant performance of laboratory works.

Simulation models make up the bulk of the program complex. They show (demonstration model) the sequence of the one or another protocol, algorithm or device step by step. In the test mode, interactive models require that the separate steps should be performed by students. Models check the correctness of these steps and the number of errors. Models form reports on the laboratory work implementation that are sent to the mail server.

Server Operating System organizes interaction of the programs connected to the server, the resources with the hardware component and the user.

HTTP-server processes the HTTP-requests that are received by the server computer, and generates HTTP responses containing the requested resources or service messages.

Databases are set of related tables that contain information for the simulation models, as well as the data about working students and teachers.

The PHP interpreter realizes the possibility of server to perform the code of PHP language, which is contained in the files of the Moodle platform and in the simulation models.

The Moodle platform includes the lecture material, the educational methodical material, test questions, and service components that implement the platform functionality.

The difference between the student`s and the teacher`s computers is only the access rights to the system components that are located on the server.

The teacher`s computer cooperates with the mail server for viewing reports. The reports are the emails that are generated and sent by the simulation models. The emails report on the results of work of students with the simulation models.

Thus, the general algorithm for the study of some entity (in this case it is the encryption algorithm and breaking the ciphers, the security protocol of network operation, the algorithms of formation and password breaking, etc., that is the first task) using the proposed hardware/firmware complex will be as follows:

1. Student is registered in the system.
2. The student has the opportunity to study the theory (if it has not been studied before) concerning the entity functioning.
3. The student activates the simulation model in the mode of "Demonstration". The model demonstrates the operation of studied protocol, algorithm step by step. Each step is commented.
4. The student activates the simulation model in the mode “Pretesting.” In the interactive mode, the student performs certain steps of the algorithm, protocol. In case of an error the model indicates the error and gives the corresponding explanations of the error reason. The student can perform such pretesting for several times.
5. The teacher gives task to the student.
6. The student activates the simulation model in the mode “Testing.” In the interactive mode, the student performs the certain steps of the algorithm, protocol. In case of an error the model indicates this error, but it does not give the explanation. The student has the opportunity of the step retry. Each error is fixed and calculated by the program.

7. At the end of testing the program evaluates the result. The mark is displayed and recorded in database.
8. The teacher has the opportunity to analyse the work of the student in the mode “Testing.”

Some master’s theses include quite difficult simulation models in the form of exe-files that are loaded to the student`s computer from the server.

To implement the second task of the study (study of the network security methods, i.e. the correct server setting, counteracting the attacks on the server, etc.) students should be provided with the testing area. However, to provide a real testing area, like for example in the Lincoln Laboratory of Massachusetts Institute of Technology is not always possible. Therefore, in a number of master's theses the educational systems that make it possible to simulate the actions of the network security manager are developed. Such systems have the client and server sides. On the client side one can simulate the actions of the violator. The server side of the system in the research process should be set up in such a way as to counteract the violator`s attacks. During research the client and the server are activated on the same computer.

Examples of the Specific Developments Performed under the Supervision of the Authors

In the master's thesis of O. Govor [12] it was developed a program complex to study the operation principles of some cryptographic generators of pseudorandom sequences, in particular, the BBS and the LFSR ones.[13]

Figure 2 represents the basic form of this complex. The complex may be in the learning or the testing mode. In the testing mode, all the objects of the basic form are blocked except the mode button.

The panel “Step by step review of the key generation” allows one selecting the encode mode with step by step review of all the actions from the key generation to the enciphering process. In this case, there appears the schematic diagram of the selected generator. The generator changes each time you press the "Next step" button. The changed blocks are highlighted.

Figure 3 represents schematic diagrams of the generators that appear on the form. In the testing mode, the student should fill the separate fields on his own. The windows that should be filled at this stage are highlighted with turquoise. If the data are incorrect it is opened the window with the word "Error !!!". The incorrect fields are highlighted with red.

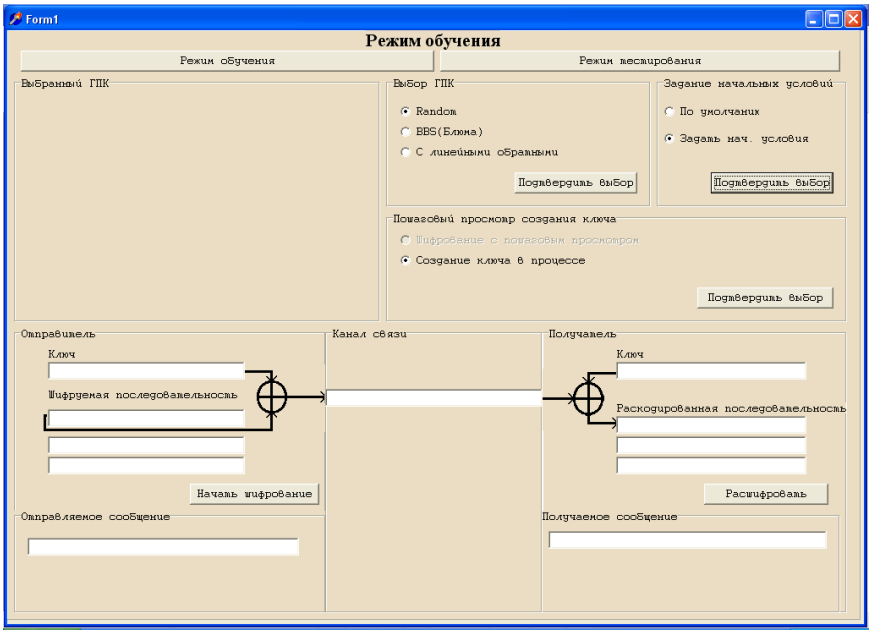

Figure 2: The basic form of the complex to study the operation principles of cryptographic generators of pseudorandom sequences.

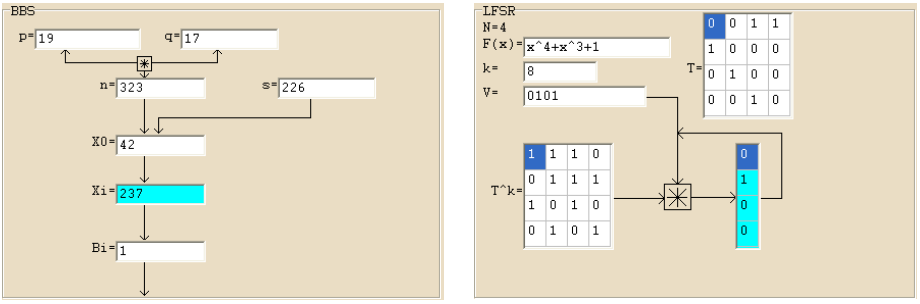

Figure 3: Representation of the generators BBS and LFSR on the form of the complex.

After completion of the enciphering process the number of errors and student`s mark are shown. These data are recorded into database and can be viewed by the teacher.

In the master's thesis of V. Shushpan [14] a program complex for studying the operation principle of the AES cipher [15] was developed. The complex can operate in the following modes:

- interactive training mode, i.e. step by step encoding of the entered message using the selected key with the corresponding comments;
- interactive testing mode, i.e. displaying the blocks of the message encryption process with the corresponding questions to each block and sending an email to the teacher with the results of successful testing.

The work with the program in training mode is illustrated in the Figure 4.

When working with the program in testing mode a modal window is opened. It shows the test questions with the corresponding encryption step in turn. The student should choose the answer (Figure 5).

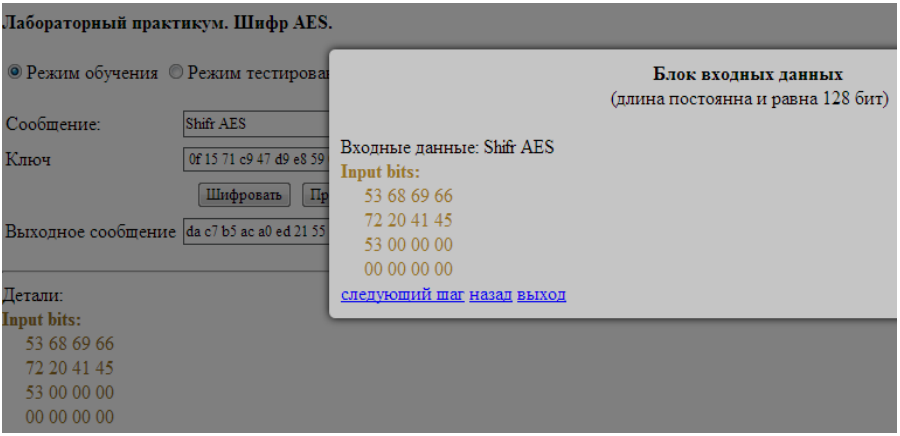

Figure 4: The next step of the simulation model of the AES cipher operation.

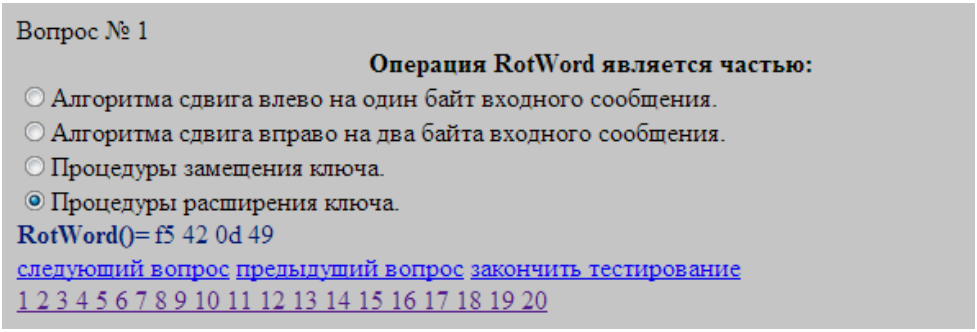

Figure 5: Example of the modal window in the testing mode.

After answering all the test questions the results are sent to the teacher.

The master's thesis of R. Teterin [16] contains the research and development of evaluation tools of re-usable passwords resistance to major attacks. Guessing attacks (a method of trial and error or brute force technique) and the dictionary attack (if the password is meaningful) can be considered the main kinds of attacks on re-usable passwords. To study the resistance and generation of re-usable passwords a special training program complex "Password Work" (see Figure 6) was developed. Its main functions are to create (generate) a re-usable password and the password test (for randomness, resistance to dictionary and guessing attacks).

Using the password generation mode of training program complex a student can freely choose the length and the alphabet and can create a pseudo-random password according to the BBS algorithm or Delphi Random.

The mode of passwords test for randomness (Figure 7) allows one performing experiments on assessing the randomness of the received password using the statistical NIST tests.[17]

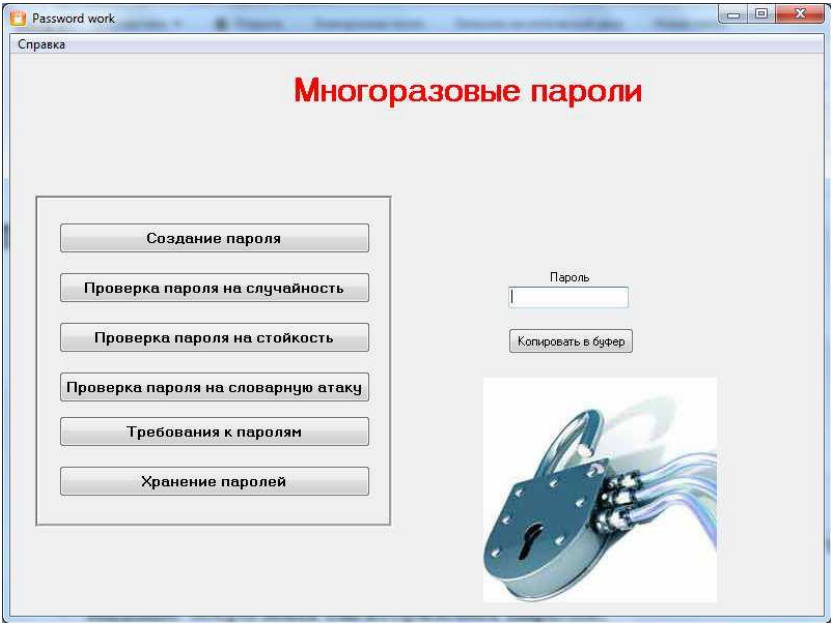

Figure 6: The main window of the training complex.

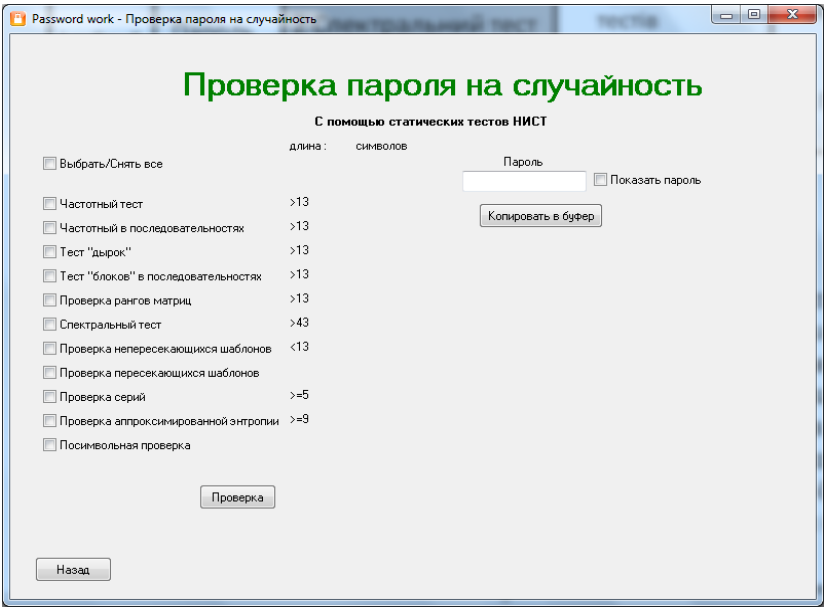

Figure 7: The window of the test for password randomness.

The mode of password test for resistance to guessing attack using the method of trial and error (see Figure 8) makes it possible to calculate the resistance indicators of the received password. These indicators are the average space and the average time of the attack.[18]. To calculate the latter one can use the value of the guessing rate, which can be determined by the training program or specified on one's own.

Using the test mode of the password resistance to the dictionary attacks one can check if the one's own meaningful password (the one that is relatively easy to remember) is included (or not included) into the dictionaries or "transported" dictionaries. It is recommended to follow the rules [19] when creating the re-usable meaningful password.

The master's thesis of E. Lapin [20] includes development of the program client-server complex of the generation and research of onetime passwords for educational purposes.

The complex consists of two sides. The client side (further client) is in the possession of user and represents the onetime password generator. Each user has the copy of the program and a set of configuration files, which contains unique settings. The server side (further server) is a user interface that allows one to simulate identification and authentication of the users. Server interface makes it possible for the user to enter his

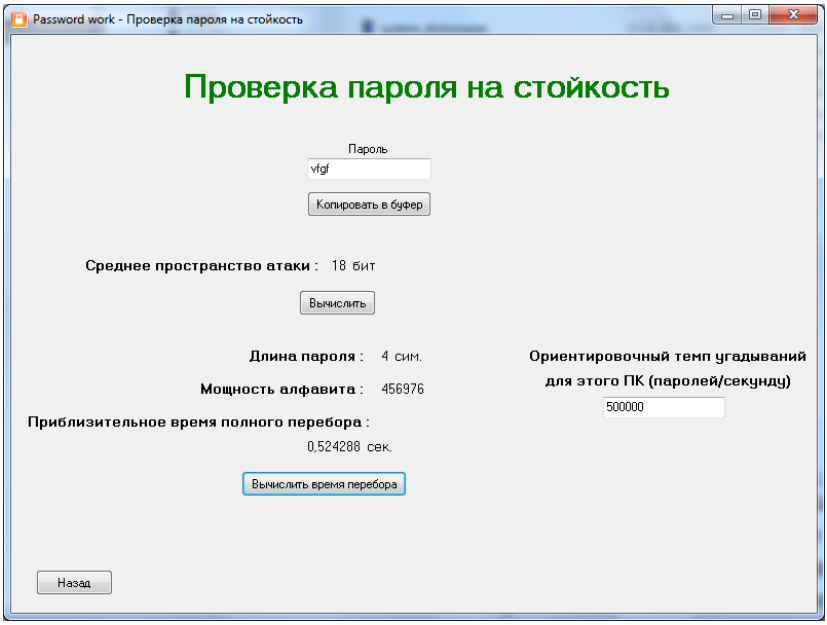

Figure 8: The window of characteristics calculation of guessing attack.

identifier (login) and one-time password. Further, on the basis of the password test the access to the information system is allowed or denied.

As it is shown in Figures 9 and 10, on the basis of the PIN-code and the base secret 1 (BS1) is constructed a key − the base secret 2 (BS2). The data block (the internal clock values) is encrypted using this secret. As a result, we get the onetime password.[19]

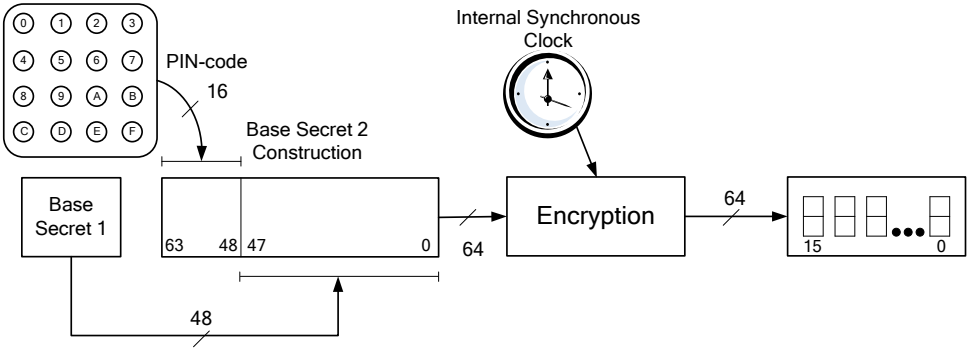

Figure 9: The scheme of organization of the client side of the complex.

The server side includes the database of users, as it is shown in Figures 10 and 11. The database includes the identifier (login) and formed base secret 2 of each user, as well as the initial setting of the internal clock for each user.[19] The user chooses login and the PIN-code and the manager enters them into the database.

After setting up the complex students can study the operation principles of systems for onetime passwords generation, investigate the influence of the time window value on the opportunity to authenticate the legitimate users and experimentally determine the rational value of the time window.

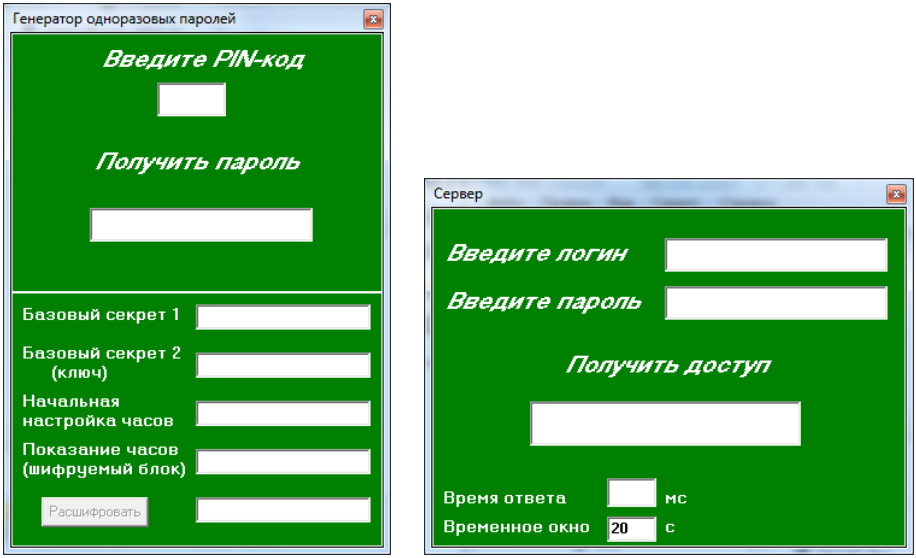

Figure 10: The windows of the client side and server side of the complex.

The master's thesis of D. Navozenko[21] includes the development of the program complex to study the authentication system based on the onetime passwords S/Key.[22] The system implements the concept of Leslie Lamport.[23] Using the complex students have the opportunity to study the operation of the S/Key system, the organization of the server database and the client configuration.

The complex is composed of two programs: the client one (onetime password calculator) and the server one (simulator of the user authentication for onetime password).

Before starting the client side of the complex (Figure 12), a student should fulfil its setting by manual editing the configuration file.

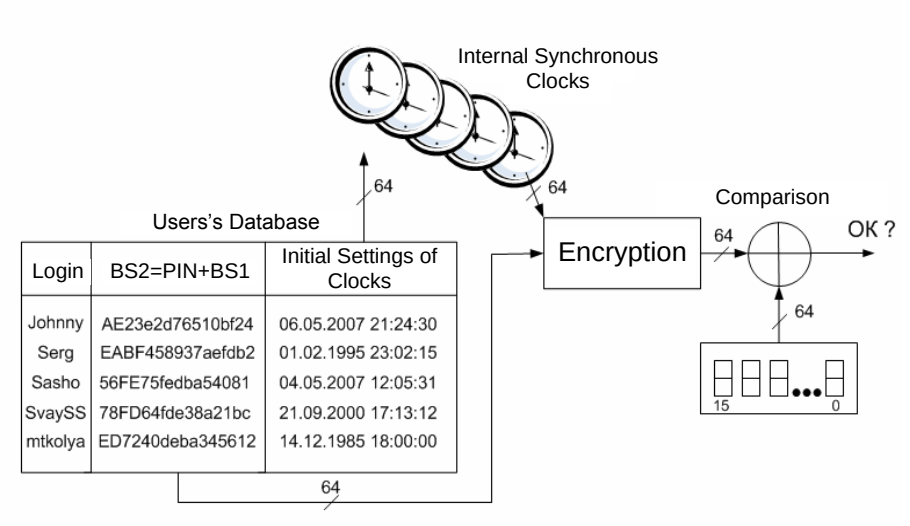

Figure 11: The scheme of organization of the server side of the complex.

After starting the program of the server side of the complex (Figure 12), a student can randomly select "mix in" or generate it. Then, figure out the response, which is the last onetime password using the client side based on the selected "mix in." The system administrator should save it on the server. The student can configure the server side of the training program complex, simulating the actions of the system manager. For this purpose, a file of user database is generated. Each line of this file corresponds to the certain user and contains certain fields.

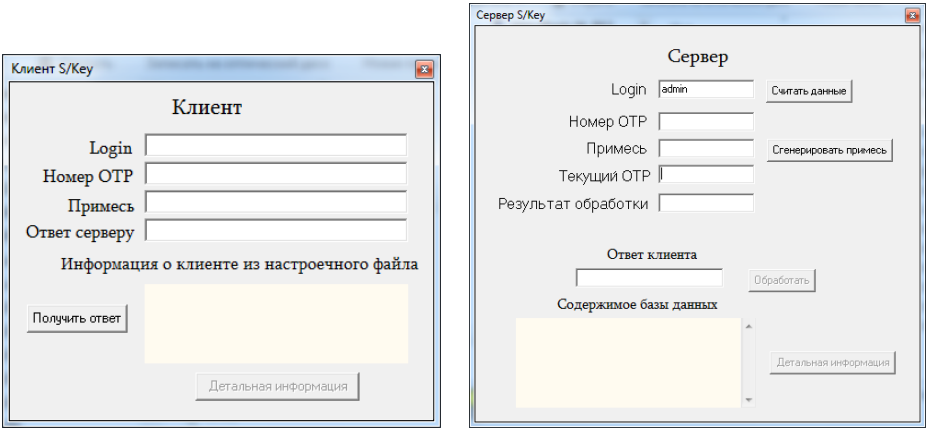

Figure 12: The windows of the client side and server side of the complex.

In addition, using the server side student can assure himself of the correctness of official information about the initial parameters for generating the client password and review the details of hashing process of the password using the algorithm MD5. The main objective of the complex operation is performing experiments on the user authentication using several onetime passwords.

Conclusions

For the practical study and research in the area of cyber security it is advisable to use the automated program complexes, which are based on interactive simulation models. The given models can operate in both the demo and the training mode. To train the skills of correct server configuration it is advisable to create the client-server simulation models. Such models can be built into the known systems of distant learning.

For the practical study and research in the area of cyber security it is advisable to use the automated program complexes, which are based on interactive simulation models. The given models can operate in both the demo and the training mode. To train the skills of correct server configuration it is advisable to create the client-server simulation models. Such models can be built into the known systems of distant learning.

The program complexes of the automated systems for practical research in the area of cyber security that were developed within the framework of master's theses are widely used in the Dnipropetrovsk National University of Railway Transport named after Academician V. Lazaryan. They are used for postgraduate education, distance education, as well as for self-study of full-time students of the specialty “Security of Information and Communication Systems.”

Many of such systems are used during laboratory works on the courses of cyber security in the university laboratories.

References

1. Stanford Cybersecurity Center, http://seclab.stanford.edu.
2. Applied Cyber Security Course – MIT, http://web.mit.edu/professional/short-programs/courses/applied_cyber_security.html.
3. CS 161, Fall 2012 Computer Security, http://www.cs.berkeley.edu/~dawnsong/teaching/f12-cs161.
4. 50+ Useful Cyber Security Online Courses You Should Explore [Updated], last updated on May 17, 2016, https://heimdalsecurity.com/blog/50-cyber-security-online-courses-you-should-know-about/
5. Cisco Networking Academy, https://www.netacad.com/about-networking-academy/packet-tracer.
6. Experiences In Cyber Security Education: The MIT Lincoln Laboratory Capture-

the-Flag Exercise, https://people.csail.mit.edu/nickolai/papers/werther-llctf.pdf.

7. Mike Ebbers, ed., *IBM Lotus Learning Management System*. *Textbook* (IBM International Technical Support Organization, 2003), - 445 pp.

8. Kerry Thompson, "Introducing the Lotus Workplace Collaborative Learning Authoring Tool," *IBM International Technical Support Organization* (2004), https://www.ibm.com/developerworks/lotus/library/LMS-LWP/.

9. Barbara Morningstar, Jeremy Schubert, and Kristine Thibeault, "WebCT: A Major Shift of Emphasis" *Technical Evolution Report* (Athabasca University, 2004). http://www.irrodl.org/index.php/irrodl/article/view/194/276.

10. Distance Learning System "Prometheus," LLC "Virtual Technologies in Education," - in Russian, http://www.prometeus.ru/actual/01_products/lms/opisanie.html.

11. Features and Specifications of Distance Education System Moodle, LLC "Open Technologies," - in Russian, www.opentechnology.ru/products/russianmoodle/futures.

12. O. Govor, *Research and Development of Hardware and Software to Protect the Serial Communication*, MR Thesis [manuscript]. Dnipropetrovsk (2011). - in Russian.

13. Martin Geisler, Mikkel Krøigård, and Andreas Danielsen, "About Random Bits," (December 2004), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.90.3779.

14. V. Shushpan, *Development of the Remote Laboratory Work on the Course "Applied cryptology,"* MR Thesis [manuscript]. Dnipropetrovsk (2015). – in Russian.

15. Christof Paar and Jan Pelzl, "The Advanced Encryption Standard," in *Understanding Cryptography, A Textbook for Students and Practitioners*, Chapter 4 (the companion web site contains online lectures on AES), (Springer, 2009).

16. R. Teterin, *Research and Development of Means of Password Authentication of Users of Information Systems*, MR thesis [manuscript]. Dnipropetrovsk (2015). – in Russian.

17. A. Rukhin, et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *NIST Special Publication* 800-22, Revision 1a. (2010), http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

18. Richard E. Smith, *Authentication: From Passwords to Public Keys* (Addison-Wesley, 2001), - 576 pp.

19. "Strong passwords," *Microsoft Technet Library* (2005), https://technet.microsoft.com/en-gb/library/cc756109(v=ws.10).aspx.

20. E. Lapin, *Research of a complex of identification of users in information systems*, MR Thesis [manuscript]. Dnipropetrovsk (2015). - in Russian.

21. D. Navozenko, *Development of a program complex of password protection by the*

principle "inquiry answer," MR Thesis [manuscript]. Dnipropetrovsk (2015). - in Russian.

22. N. Haller, "The S/KEY One-Time Password System," *RFC 1760* (Bellcore, 1995), http://tools.ietf.org/html/rfc1760.

23. Leslie Lamport, "Password Authentication with Insecure Communication," *Communications of the ACM* 24, no. 11 (1981): 770-772, https://doi.org/10.1145/358790.358797.

About the Authors

Igor ZHUKOVYTS'KYY and Denis OSTAPEC are with the Department of "Electronic computational machines" at the Dnipropetrovsk National University of Railway Transport named after Academician V. Lazaryan, Lazaryna str. 2, 49010 Dnipropetrovsk, Ukraine. E-mail of the corresponding author: ivzhuk@mail.ru.