DOI: https://doi.org/10.30837/csitic52021232201

Model for Providing the Second Factor of Authentication Into Authentication Services with Centralized Account Databases

Bohdan Rezanov[1],
Anna Semenova[1],
Inna Petrovska[1]
Tetiana Fesenko[2]

[1]National Technical University «Kharkiv Polytechnic Institute», Kharkiv, 2, Kyrpychova str.,Ukraine
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,

Abstract. *The study developed a model for providing the second factor of authentication into authentication services with centralized account databases.This paper focuses on developing a model for providing the second factor of authentication into authentication services with centralized account databases.The paper describes the modeling methods, the modeling method based on PERT networks is described in detail. Is described the model of the process of integration of the second factor in authentication services with centralized account databases on the basis of mathematical formalization technology based on PERT, the sequence diagram of modules interaction at change password in the external target system (authentication service with centralized account database), PERT diagram representing time spent for the execution of each module on a certain stage.*

Keywords: *two-factor authentication, modeling, Active Directory, PERT, Java Microbenchmark Harness.*

I. Introduction and Problem statement

Over the past few years, the number of large-scale attacks and data breaches has increased significantly, and the need for additional layers of security has increased. Research has shown that the most popular way to protect your digital accounts is by using a password.

Cybercriminals' tools are constantly improving, and cases of data theft by well-known companies are only becoming more frequent, so one level of protection may often not be enough. The easiest way to create an extra layer of security for your accounts is with two-factor authentication.

Active Directory is a distributed database that contains all objects in a domain. Domain environment Active Directory is a single point of authentication and authorization of users and applications throughout the enterprise [1].

Research has shown that Active Directory does not have two-factor authentication support.

Modeling is a cognitive method of creating and exploring models. The theory of replacing original objects with a model object is called modeling theory.

The main stages of modeling are:

- problem statement;
- model development, analysis, and study of the problem;
- computer (full-scale, physical) experiment;
- analysis of simulation results.

Graph approaches include GERT nets, PERT nets, CPM, Petri nets. Each of them has its own advantages and disadvantages.

Thus, the task of developing a model for providing the second factor of authentication into authentication services with centralized account databases on the basis of the technology of mathematical formalization based on the PERT network becomes urgent.

PERT allows for possible fluctuations in the timing of each operation and analyzes their impact on the completion of the project as a whole.

Benefits of PERT:

- provides a graphical display of the project and its main activities;
- allows you to set a range of duration for each type of activity;
- gives the opportunity to obtain information about the expected time of completion of the project, provides an assessment of the likelihood of completion of the project before the specified date;
- identifies actions that have a spare time and therefore their delay will not affect the duration of the project as a whole;
- identifies activities on the critical path that require close monitoring, as they affect the total time to complete the project [2].

II. Problem solution and Results

Let us simulate the processes of interaction between modules when performing a password change operation in an external target system.

A general view of the process in the form of a sequence diagram of the interaction of modules is shown in Figure 1.

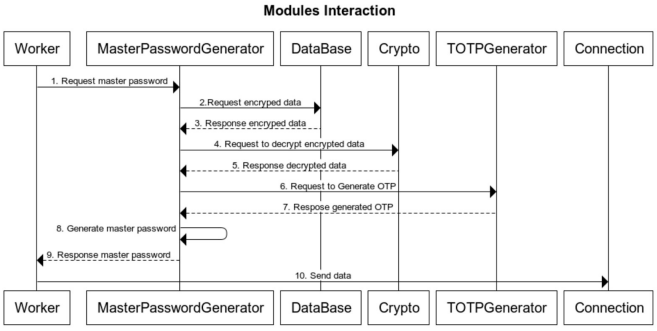

Figure 1. Modules iteractions

To obtain data for the formation of a PERT diagram, it is necessary to test the operation of each module.

Researches have shown that to conduct performance tests for applications written in the JAVA language, it is advisable to use the Java Microbenchmark Harness (JMH) [3].

The requirements for testing the system set during the experiment determined the condition for evaluating the performance of each module separately using Mode.AverageTime. The accuracy of the obtained execution time should be presented in milliseconds, based on 1000 iterations.

The test results are shown in Figure 3:

Benchmark	Mode	Cnt	Score		Error	Units
Benchmark.MasterPasswordGenerator(1 step)	avgt	1000	150.541	±	0.045	ms/op
Benchmark.DataBase	avgt	1000	1278.594	±	0.129	ms/op
Benchmark.MasterPasswordGenerator(2 step)	avgt	1000	152.031	±	0.544	ms/op
Benchmark.Crypto	avgt	1000	1354.976	±	0.093	ms/op
Benchmark.MasterPasswordGenerator(3 step)	avgt	1000	153.640	±	0.490	ms/op
Benchmark.TOTPGenerator	avgt	1000	341.390	±	0.012	ms/op
Benchmark.MasterPasswordGenerator(4 step)	avgt	1000	981.409	±	0.310	ms/op
Benchmark.Worker	avgt	1000	398.348	±	0.011	ms/op
Benchmark.Connection	avgt	1000	3641.348	±	0.489	ms/op

Figure 2. Test results

Based on the test results, a PERT diagram of the interaction of the modules with the obtained values was generated.

Figure 3. PERT diagram

The presented PERT diagram represents the time taken to complete each module at a specific stage.

III. CONCLUSIONS

The conducted research of the model showed that time expenditures confidently fit into the requirements defined by international standards for two-factor authentication procedures [4].

In the future, it is advisable to carry out comparative researches of the developed model for integrating the second factor into authentication services with centralized user bases in use with other existing models.

REFERENCES

[1] Free implementation Active Directory // https://www.oslogic.ru/blog/svobodnaya-realizatsiya-active-directory/

[2] Methods and techniques of project management in the field of industrial production. Market economy problems. – 2017. - № 3. – C. 17–24.

[3] Java Microbenchmark Harness (JMH) // https://github.com/openjdk/jmh

[4] Y.2720 : NGN identity management framework // https://www.itu.int/rec/T-REC-Y.2720-200901-I

[5] production. Market economy problems. – 2017. - № 3. – C. 17–24.

[6] TOTP: Time-Based One-Time Password Algorithm // https://tools.ietf.org/html/rfc6238

[7] Bohdan Rezanov, Galina Cherneva, Maksym Bartosh. Method for providing two-factor authentication in operating systems working with authentication services with centralized account databases in telecommunication networks. Mechanics Transport Communications. – 2021. - volume 19, issue 1. – article № 2065.