A Generalized Net Model for Accessing Information Resources in a Secure Environment

Miroslav Kochankov
Bulgarian Defense Institute
„Professor Tsvetan Lazarov“
Sofia, Bulgaria
m.kochankov@armf.bg

Rosen Iliev
Bulgarian Defense Institute
„Professor Tsvetan Lazarov“
Sofia, Bulgaria
r.iliev@di.mod.bg

Abstract. **The purpose of the study is to describe and present the process of accessing information resources in a secure military computer network as generalized net model. A simulation of the model was carried out using specialized software for working with generalized nets - GN IDE, and the most important results are visualized in the report.**

Keywords: Generalized net, modeling, military network, access control.

I. Introduction

Any secured military computer network that store and process secured information or provide access to secured services requires incensement of security measures. [5], [8], [14].

The access control to the network and provided resources is carried out in accordance with the regulatory documents and modern technologies. [9], [10], [11], [13].

II. Materials and Methods

One approach to provide secured and reliable access to a secured military computer network is the mechanism of personal smart card and personal access code [15]. The smart card has an integrated programmable verification chip that contains the necessary information about the card holder to guarantee access to the system's resources. The personal access code confirms the authenticity of the cardholder and validates access to the system [15]. Access to the system is granted after reading the information from the smart card and entering a valid pin code, otherwise access is denied and the system generates an error message.

When the user gets access to the system and make a request to the certain service provided by the system, it checks the user clearance, if the check is successful the system makes a check for access to the service performed on a need-to-know basis. In accordance to this principle, the user's access is limited only to that information that is necessary for the performance of official duties or for the performance of a specific task [6]. If the specified checks are passed, the user has access to the service if it is available, otherwise access is denied and the system generates an error message.

The generated errors are fed into the network analysis and monitoring module, where an analysis of the errors and possible security issues in the system is performed.

One of the possible approaches for describing the process is the generalized netus created by K. Atanasov [1], [2], [3], they allow a detailed description of the individual steps and creation of an interaction model.

The usage of intuitionistic fuzzy sets in the process description allows a detailed evaluation of possible failures of the system access control.

Five transitions are used in the present work to represent the process of accessing services in a secure military computer network.

The scheme of the process represented by a generalized net is shown in Fig1.

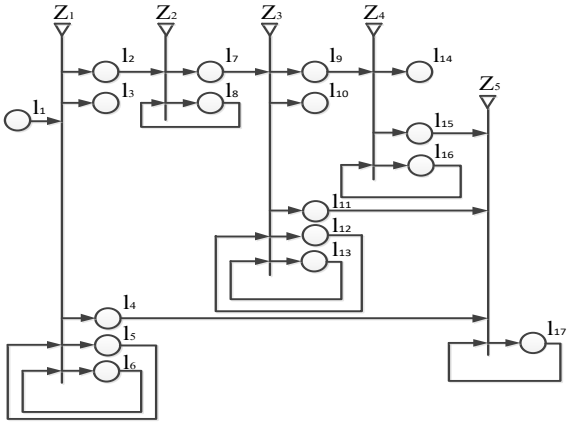

Fig.1 Generalized net model

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol2.8034

Tokens into the net:

- α - users;
- β – smart cards data base;
- γ – PIN codes data base;
- δ – list of services;
- ε – clearances data base;
- ϵ – need to know data base.

Generalized net is presented by a set of transitions E = {Z_1, Z_2, Z_3, Z_4, Z_5}, where transitions describe the following processes:

Z_1 – User authorization
Z_2 – Service request / network resource/
Z_3 – Services access level
Z_4 – Services access confirmation
Z_5 – Errors evaluation and analysis

Transition Z_1 - User authorization

$Z_1 = \{l_1, l_5, l_6\}, \{l_2, l_3, l_4, l_5, l_6\}, r_1, \vee(l_1, l_5, l_6)$, where:

l_1 – user
l_2 – authorized user
l_3 – exit
l_4 – authorization failed
l_5 – pin codes data base
l_6 – smart cards data base

$r_1 =$

	l_2	l_3	l_4	l_5	l_6
l_1	F	F	F	F	T
l_5	$W_{5,2}$	$W_{5,3}$	$W_{5,4}$	T	F
l_6	F	$W_{6,3}$	$W_{6,4}$	$W_{6,5}$	T

T (true) – possible transition, F (false) – no possible transition

$W_{5,2}$ – authorized user
$W_{5,3}$ – the pin code is not valid
$W_{5,4}$ – pin code validation failed
$W_{6,3}$ – the smart card is not valid
$W_{6,4}$ – smart card validation failed
$W_{6,5}$ – the smart card is valid

All user credential checks are performed in this transition - Z_1 . At position l_6 the system checks smart card validity, if it is valid, the system checks pin code at l_5. If the smart card or pin code are not valid the tokens go to exit, position l_3. If both checks are valid tokens go to position l_2.

Transition Z_2 – Service request

$Z_2 = \{l_2, l_8\}, \{l_7, l_8\}, r_2, \wedge(l_2, l_8)$

l_7 – authorized user
l_8 – services provided by the system

$r_2 =$

	l_7	l_8
l_2	F	T
l_8	T	F

Transition Z_3 - Services access level

$Z_3 = \{l_7, l_{12}, l_{13}\}, \{l_9, l_{10}, l_{11}, l_{12}, l_{13}\}, r_3, \vee(l_7, l_{12}, l_{13})$

l_9 – authorized user
l_{10} – exit
l_{11} – validation failed
l_{12} – „need to know" data base
l_{13} – clearances data base

$r_3 =$

	l_9	l_{10}	l_{11}	l_{12}	l_{13}
l_7	F	F	F	F	T
l_{12}	$W_{12,9}$	$W_{12,10}$	$W_{12,11}$	T	F
l_{13}	F	$W_{13,10}$	$W_{13,11}$	$W_{13,12}$	T

$W_{12,9}$ – authorized user with services access
$W_{12,10}$ – the user has no access to the requested service
$W_{13,10}$ – the user has no valid clearance
$W_{13,11}$ – error occurred
$W_{13,12}$ – valid clearance

At this transition (Z_3) are performed users service access level checks. At position l_{13} the system checks user clearance, if it is valid and at the same level as required service, the system checks users request according „need to know" principle at l_{12}. If the clearance or „need to know" parameters are not the same tokens go to exit, position l_{10}. If both checks are valid tokens go to position l_9.

Transition Z_4 - Services access confirmation

$Z_4 = \{l_9, l_{16}\}, \{l_{14}, l_{15}, l_{16}\}, r_4, \vee(l_9, l_{16})$

l_{14} – exit/service provided
l_{15} – requested service is not available
l_{16} – available services

$r_4 =$

	l_{14}	l_{15}	l_{16}
l_9	F	F	T
l_{16}	$W_{16,14}$	$W_{16,15}$	F

Transition Z_5 - Errors evaluation and analysis

$Z_5 = \{l_4, l_{11}, l_{15}, l_{17}\}, \{l_{17}\}, r_5, \vee(l_4, l_{11}, l_{15}, l_{17})$

l_{17} – errors evaluation and analysis

$r_5 =$

	l_{17}
l_4	T
l_{11}	T
l_{15}	T
l_{17}	T

In transition Z_5 – Evaluation and analysis of errors, an evaluation of possible errors during system operation is carried out. Initially, in the absence of information coming from any of the transition input positions l_4,l_{11},l_{15},l_{17}, the values are <0,0>>

When k≥0 then (k+1) grade is based on previous grades according to:

$$< \mu_{k+1}, \nu_{k+1} > = \frac{\mu_k + \mu}{k+1}, \frac{\nu_k + \nu}{k+1}$$

When k≥0, grade is calculated based on the previous grades, where <μ_k,ν_k> is the previous grade and <μ,ν> is the latest grade.

III. Results and Discussion

Model simulation and results

The simulation of the proposed model was performed with the GN IDE (Generalized Nets Development

Environment) [4],[7],[12]. The software allows graphical representation of the model and track the model operation, as well as possible errors that occur. In the presented model, it is assumed that on every tenth step starts a new simulation cycle.

The rules for performing the simulation are set in the program code, with a 90% probability of passing the set checks, 7% of failed attempts and a 3% probability of errors.

Fig.2 represents the initial state of the simulation, l_1 is in the initial position before entering and activating transition Z_1.

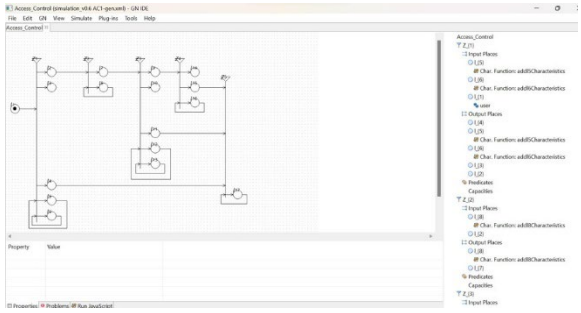

Fig.2. Initial state

Fig. 3 shows the final state of the simulation, where the characteristics of tokens that has successfully passed all set checks.

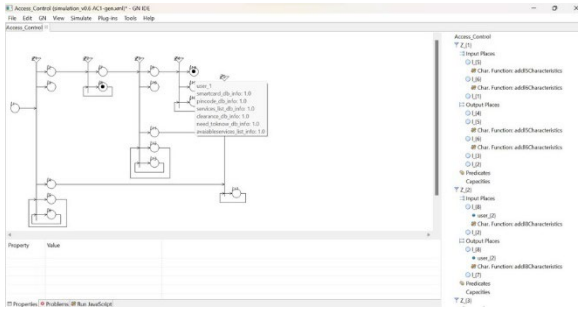

Fig.3. Final state

Possible errors that occur during the simulation.

Performing a simulation of the proposed generalized net model with the GN IDE software requires N number of runs and passes through the model to generate different results. Two types of errors are possible in presented model, known type and unknown type. Known type errors for example are invalid smart card, wrong pin code, unavailable service user does not have valid clearance. Errors of a known type generate an error message and go to exit place. For errors of unknown type, tokens go to the error analysis block.

Fig. 4 shows an error where the user does not have access to the requested service according to the "need to know" principle.

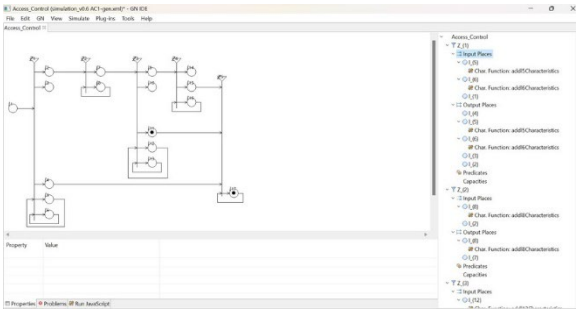

Fig.4. The user does not have access according to the "need to know" principle.

Fig. 5 shows an error where there is a pin code problem.

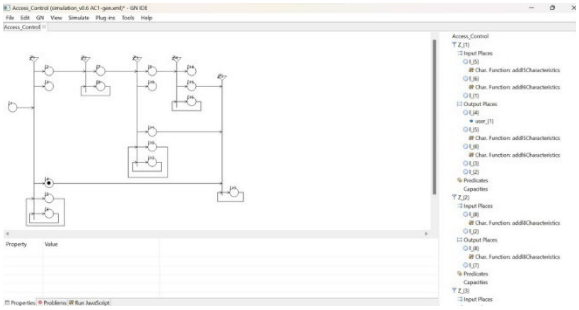

Fig.5. Pin code error

V. CONCLUSION:

At this article is presented generalized net model describing the access control military computer network. Ensuring secure and reliable access control is a priority task to prevent unregulated access to information and services provided by the network.

The model can be used independently or like a component of other generalized model with additional security parameters. This model can help examination, analyze and optimization of access control to secured military network.

ACKNOWLEDGEMENTS:

This publication was financed by the Ministry of Education and Science in implementation of the National Science Program “Security and Defence”, adopted with PMC № 731 of 21.10.2021 and according to Agreement № Д01-74/19.05.2022.

REFERENCES

[1]. Atanassov K. Theory of Generalized nets (an algebric aspect). AMSE Review, 1, №2, 27-33, 1984.
[2]. Atanassov, K.(ed.). Applications of Generalized nets. World Scientific, Singapore, New Jersey, London 1993.
[3]. Atanassov K, Generalized Nets, World Scientific, Singapore, New Jersey, London 1991
[4]. Angelova, N, Todorova, M., Atanasov, K. GN IDE Implementation, improvements and algorithms. pp 69.411-420, 2016
[5]. Boyanov, P., Using a specialized software for comprehensive monitoring the suspicious states in computer networks, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 6, 2014, pp. 148-154
[6]. Classified Information Protection Act, Ch1, Art3, (2), 2023

[7]. Dimitrov, D.G. GN IDE – A software tool for Simulation with generalized nets. Proceedings of Tenth International Workshop on Generallized nets, Sofia, 2009, pp 70-75.

[8]. Hristov, Hr., Boyanov, P., Trifonov, T., Approaches to identify vulnerabilities in the security system of the social organization and computer resources, a refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 5, 2014, pp. 101-107.

[9]. Kolev, A., P. Nikolova, Instrumental Equipment for Cybe-rattack Prevention, Information & Security: An International Journal 47, no. 3 (2020): 285-299. https://doi.org/10.11610/isij.4720

[10]. Александрова, К., Ив. П. Иванов, Архитектура на пасивна бистатична радарна система базирана на DVB-T сигнали и софтуерно-дефинирана платформа, "Сборник доклади от международна научна конференция "Хемус 2016", стр. III-193 – III-201, ISSN 1312-2916, 2016 г.

[11]. Александрова, К., Ив. П. Иванов, Перспективни радари срещу електронните заплахи на съвременното бойно поле. "Сборник доклади от международна научна конференция "Хемус 2016", стр. III-202 – III-210, ISSN 1312-2916, 2016 г.

[12]. Димитров, Д. Графична среда за моделиране и симулация с обобщени мрежи. 2021 г.

[13]. Спасов, Св. Международни академични програми и модели за обучение по противодействие на корупцията и приложението им в УНСС. Научни трудове на УНСС, 69-95 стр., 2022 г.

[14]. Спасов, Св. Европейска архитектура за сигурност. Книга, Издателство на УНСС, ISBN: 978-954-644-340-3, 2012 г.

https://www.iogear.com/product/GSR205/ – last seen 06.02.2024.