Efficiency of lattice-based security mechanisms supporting public tasks on digital integration platforms

J. WILK
jaroslaw.wilk@wat.edu.pl

Military University of Technology, Faculty of Cybernetics
Kaliskiego St. 2, 00-908 Warsaw, Poland

Integration platforms are the solution increasingly used by the public administration in Poland in order to make public tasks available and implement the tasks on these platforms (in the form of electronic services). In earlier publications, the author proposed a mathematical model based on lattice mechanisms that ensures the secure provision of these services (from a confidentiality perspective). In the following publication the author's model was cited (its main elements) and then the analysis of a time efficiency of the approach with using lattice mechanisms with the general model was performed. The efficiency examined concerned both the implementation of public tasks – and more precisely the verification of their correctness from the security perspective before the implementation as well as concerned an expansion of the process of handling the public task. The author has demonstrated that in both cases it is appropriate to use the lattice solution, as its time efficiency is better.

Keywords: public tasks execution, efficiency, security model, lattice based model.

DOI: 10.5604/01.3001.0015.8607

1. Introduction

Digital platforms are increasingly the environment for producing, interacting and sharing electronic services. One of the main areas of application of platforms of this kind is the implementation of processes for the handling of public tasks [8] provided by the public administration electronically. In its earlier publications [5, 6, 7], the author detailed mathematical models of processes for the handling of public tasks in the environment of electronic platforms, with particular emphasis on ensuring confidentiality, as the basic security feature when executing them. The proposed approach uses the lattice theory and is built in line with the concept of multilateral frameworks of interoperability. This solution was then used by the author as the basis of a design method, the application of which will ensure the creation of security mechanisms with formally and unambiguously confirmed properties. The results of these considerations are in the process of being published and reviewed as part of the author's ongoing doctoral dissertation. Notwithstanding the aforementioned use of the developed models, the author decided to perform an additional check of the efficiency of the approach used, based on the lattice model. It has been demonstrated under which conditions time efficiency using the lattices will be greater during the implementation of electronic services. In addition, a significant advantage was identified for the use of the lattice mechanism and equivalence classes in case of extension of the model by, for example, additional enforcements.

Chapter 2 introduces briefly into the model developed and discussed in previous publications [5, 6, 7]. Subsequently, **Chapter 3** presents a theoretical discussion and efficiency assessment of the process of checking the correctness (from a security perspective) of handling the public task on electronic platforms. The approach with and without the use of the lattice model is compared. In addition, an analysis of efficiency related to the recalculation of the model as a result of its extension is also performed. **Chapter 4** makes a practical comparison (using graphs based on a calculation example) of efficiency of the models discussed in the previous chapters, with and without the use of the lattices. **Chapter 5** provides a summary and conclusions of the results.

2. A lattice model for controlling the security of handling public tasks in the electronic platforms' environment

A lattice model for controlling the security of handling public tasks in the electronic platforms' environment is based on the security control model of domain platforms and the super lattice of the trans-domain platform built on the basis of three aspect lattices. Presented lattice security model is based on [2] and [4] where they were used accordingly for data flow and database security. In [1] interoperability model and security concepts to protect information systems of public admiration were presented.

The security control model for disciplinary platforms (SM) consists of data and service security control models with *HF* and *BF* functions.

$$SM = \langle P, D, Q, R, T, E, B, \rho, \tau, \delta, VF \rangle \quad (1)$$

where:

- P – the collection of entities $P = \{p_1, p_2, \dots, p_i, \dots, p_I\}$,
- D – the collection of data units $D = \{d_1, d_2, \dots, d_m, \dots, d_M\}$,
- Q – the collection of confidentiality classes $Q = \{q_1, q_2, \dots, q_h, \dots, q_H\}$,
- R – the collection of operations $R = \{r_1, r_2, \dots, r_n, \dots, r_N\}$,
- T – collection of scopes of operations $T = \{t_1, t_2, \dots, t_g, \dots, p_G\}$,
- E – the collection of services $E = \{e_1, e_2, \dots, e_l, \dots, e_L\}$,
- B – the collection of categories of permissions $B = \{b_1, b_2, \dots, b_f, \dots, b_F\}$,
- ρ – flow relationship,
- τ – operation relationship,
- δ – the service launch relationship,
- VF – the functions of the model:

$$VF = \langle HF, BF \rangle \quad (2)$$

HF and BF functions are described in detail in previous publications [5] and are not essential for further efficiency analysis and are therefore not re-cited. When analysing the relationships of flow $\boldsymbol{\rho}$, operations $\boldsymbol{\tau}$ and the services' launch $\boldsymbol{\delta}$, it should be noted that if the condition of partial arrangement of the collection of confidentiality classes $\boldsymbol{Q}$, the collection of operations scope $\boldsymbol{T}$ and the collection of categories of permissions $\boldsymbol{B}$ is met, it was possible to use the lattice theory. This significantly improved the process of security verification and allowed for the inclusion, under certain formal conditions, of domain security rules when determining the "resultant" of the security rule for handling the public task with the usage of a properly understood electronic trans-domain (integration) platform.

Flow relationship $\boldsymbol{\rho}$ (feedback-based, transitory and asymmetric) creates the lattice for the flow $\boldsymbol{QL}$ by partial arrangement of the collection $\boldsymbol{Q}$. There is the supremum and the infimum for each pair of confidentiality classes from the collection $\boldsymbol{Q}$.

The flow lattice QL is defined in the following way:

$$QL = \left(Q, \rho, \oplus^Q, \otimes_Q\right) \quad (3)$$

where:

- Q is the partially arranged collection,
- $Q = \{q_1, q_2, \dots, q_h, \dots, q_H\}$,
- ρ is the relationship of the partial arrangement,
- $\oplus^Q$ the operator to set the supremum of its arguments,
- $\otimes_Q$ the operator to set the infimum of its arguments.

Operation relationship $\boldsymbol{\tau}$ (feedback-based, transitory and asymmetric) creates the lattice for the operation $\boldsymbol{TL}$ by partial arrangement of the collection $\boldsymbol{T}$. There is an upper and a lower limit for each pair of operation scopes from the collection $\boldsymbol{T}$.

The operation lattice TL is defined in the following way:

$$TL = (T, \tau, \oplus^T, \otimes_T) \quad (4)$$

where:

- T is the partially arranged collection,
- $T = \{t_1, t_2, \dots, t_g, \dots, t_G\}$,
- τ is the relationship of the partial arrangement,
- $\oplus^T$ the operator to set the supremum of its arguments,
- $\otimes_T$ the operator to set the infimum of its arguments,

The service launch relationship $\boldsymbol{\delta}$ (feedback-based, transitory and asymmetric) creates the lattice for the launch of $\boldsymbol{BL}$ services by partial arrangement of the collection $\boldsymbol{B}$. There is the supremum and the infimum for each pair of the categories of permissions from the $\boldsymbol{B}$ collection.

The lattice of the BL launch category is defined as follows:

$$BL = (B, \delta, \oplus^B, \otimes_B) \quad (5)$$

where:

- B is the partially arranged collection,
- $B = \{b_1, b_2, \dots, b_f, \dots, b_F\}$,
- δ is the relationship of the partial arrangement,
- $\oplus^B$ the operator to set the supremum of its arguments,
- $\otimes_B$ the operator to set the infimum of its arguments.

The complete model of the data and service security control consists, with the concept described here, of three lattices:

- The flow lattice: $QL = (Q, \rho, \oplus^Q, \otimes_Q)$ [relates to data]
- The operation: $TL = (T, \tau, \oplus^T, \otimes_T)$ [relates to operation]
- The categories of permissions: $BL = (B, \delta, \oplus^B, \otimes_B)$ [relates to services].

Such mathematical models in the form of lattices would be designed both for individual domain platforms and for trans-domain (integration) platforms – and at that time they would be called "super-lattices". These super-lattices would separately cover the three aforementioned aspects of security protection of the trans-domain platform.

The definition of enforcement that may occur on a given electronic platform is also important from the perspective of further considerations – they form a collection *W*:

$$W = \{w_1, w_2, \dots, w_n, \dots, w_N\} \quad (6)$$

where: *N* is the number of enforcements types that may occur on a given electronic platform.

The sequence of enforcements, defined by the scheme for handling the public task, defines the process of handling the public task unambiguously.

The enforcements are in the form of ordered triplets:

$$(d_m, r_n, e_l) \in D \times R \times E \quad (7)$$

Of course, the implementation of a specific public task (from *Z*) initiated by one of the entities requires the creation of a specific sequence of enforcements, which indicate one of the data units (from *D*), one of the operations (from *R*) and one of the electronic services (from *E*). And it is only a sequence of such enforcements that will make it possible to complete the process of handling the task.

However, for the proper functioning of the security mechanism, it is fully sufficient to see enforcements as the below-shown organized triplets:

$$(q_h, t_g, b_f) \in Q \times T \times B \quad (8)$$

This is sufficient, since the security protection rules for electronic platforms refer to confidentiality classes, scopes of operations and categories of authorisations and not to their specific examples. The specific functions allowing for the above transformations have not been cited as they are not relevant from the perspective of the topic of the paper. Some more details about integration platforms models and practical implementations that will help to understand the concept better can be found in [3].

3. Efficiency of the lattice security mechanisms

In order to verify the correctness (from the security point of view) of the process of handling the public task, it is necessary to verify whether each enforcement $(w_1, w_2, \dots, w_i, \dots, w_I) \epsilon \Psi$ meets the security limitations of the given model. Following the transformation of enforcements into a sequence of triples (d_m, r_n, e_l) (as considered in Chapter 2) – of requests for flow, access to data units, and launching the services, it is necessary to check whether they are members of the relations of, respectively:

- ρ – the flow,
- τ – the operation,
- δ – the services' launch.

For "I" enforcements, "I" checks must be made on these relationships. More precisely, the total number of checks would be $3 * I$, if they were to be considered from the lower level of requests for flow, access to data units and execution of services, but for the sake of simplification further consideration would be carried out on a more general level of enforcements – so "I" checks.

Due to the usage of lattice mechanisms, the number of necessary checks can be significantly reduced by dividing the collection Ψ into J of the total sub-collections (equivalence classes), which include all the different enforcements present in Ψ. Then, instead of direct checks on

the relations ρ, τ or δ it is possible for the lattice operators to operate in advance (supremum and infimum) and to obtain a single element to represent this sub-collection. Due to this approach, only a representative of the equivalence class will be subject to verification, not all elements, which will allow to reduce the number of necessary checks to the number of divisive sub-collections of J. From the perspective of further considerations, it is crucial to establish that the equivalence collections will be created if at least one request: flow, access to data units or activation of services (being a triple of the enforcement – (d_m, r_n, e_l)) concerns the same element.

As a result, we obtain a division into $\{\widetilde{\Psi}_1, \widetilde{\Psi}_2, \dots, \widetilde{\Psi}_j, \dots, \widetilde{\Psi}_J\}$ of separate sub-collections where the usage of the lattice operators (supremum and infimum) will be necessary. From the point of view of efficiency, it is not relevant which of the operators $(\oplus^Q, \otimes_Q, \oplus^T, \otimes_T, \oplus^B, \otimes_B)$ of three different lattices will be used, therefore the fact that either of them is used is marked by a symbol $\widehat{\oplus}$.

In order to determine the efficiency of the lattices, an efficiency index ε was introduced, which will depend, in the general case, on the relative coefficient of the execution time of the I checks in the aforementioned relations and the time necessary for the creation of J equivalence classes, the triggering of the lattice operators and the execution of J checks in these relations. When determining the execution times of individual operations, it is possible to determine the coefficient of efficiency of the usage of lattices ε, where:

- τ_u – time of creation of a collection of equivalence classes,
- τ_R – time of execution of one check for three relations ρ, τ and δ,
- τ_o – time of one activation of the operator $\widehat{\oplus}$ on elements of requests,
- I – number of enforcements in the existing process,
- J – number of equivalence classes of the process.

Time of the examination of the correctness Ψ of the process with the usage of lattices – τ_{KR}:

$$\tau_{KR} = \tau_u + \tau_R \cdot J + \tau_o \sum_{j=1}^{J} \left(\left|\widetilde{\Psi}_j\right| - 1\right) = \\ = \tau_u + \tau_R \cdot J + \tau_o \left(\sum_{j=1}^{J} \left|\widetilde{\Psi}_j\right| - J\right) \qquad (9)$$

From the conditions defining the method of division:

$$\sum_{j=1}^{J} \left|\widetilde{\Psi}_j\right| = N \leq I \qquad (10)$$

so:

$$\tau_{KR} = \tau_u + \tau_R \cdot J + \tau_o (N - J) \leq \\ \leq \tau_u + \tau_R \cdot J + \tau_o (I - J) \qquad (11)$$

Time of examination the correctness of the process of implementation the public task with the chosen general model (with no lattices used) – τ_{OG}:

$$\tau_{OG} = \tau_R \cdot I \qquad (12)$$

The lattice usage efficiency index, as the ratio of the times τ_{OG} to τ_{KR}:

$$\varepsilon = \frac{\tau_{OG}}{\tau_{KR}} = \frac{\tau_R \cdot I}{\tau_u + (\tau_R - \tau_o) J + \tau_o N} \qquad (13)$$

The primary gain in efficiency is obtained by replacing process Ψ with the collection $\widetilde{\Psi}$ (i.e. by eliminating multiple checks for the same enforcements). If this profit is eliminated, that is to say I = N, the use of lattices makes sense, from the point of view of time savings, only if $\tau_R \rangle\rangle \tau_o$ or at least $\tau_R \rangle \tau_o$.

A significant benefit from the application of the lattice mechanism and equivalence classes can be seen when new enforcements (triplets: service, operation, data unit) need to be added to the task handling process.

As part of the estimation of the efficiency of the mechanism under the conditions of adding new enforcements to the process, two extreme cases (in terms of the time of considering the modification(s)) will be considered. In the first, most favourable case, the expansion of the process results from the addition of a new service. Assuming that in the model at the previous stage of activity the J classes of equivalence based on services were distinguished, the added triplets can be classified as a new, next class of equivalence with number J + 1. Then, by substituting into equation (11) the zero τ_u (the time of creation of the collection of equivalence classes), since the modification of the process automatically caused the creation of an additional equivalence class (with number J+1), we obtain a relation proportional to the number of execution of the operator $\widehat{\oplus}$ for the new enforcements (belonging to the class with number J+1),

$$\tau_{KR} = \tau_R + \tau_o (N^O - 1) \qquad (14)$$

where:
N^O – the number of "new" enforcements (triples added).

The time τ_u of creation of a collection of equivalence classes is not present (the class is defined within the scheme). The efficiency shall be:

$$\varepsilon = \frac{\tau_R(I+N^O)}{\tau_R+\tau_o(N^O-1)} \quad (15)$$

If the various enforcements from N^O relate to different enforcements, the number of enforcements assigned to the individual equivalence classes (each class includes another service) may be designated as N_j^O, where $0 \leq N_j^O < N^O, j \in \{1,2,\dots,J\}$ and $\sum_{j=1}^{J} N_j^O = N^O$. The modification applies, of course, to the classes for which $N_j^O > O$ i.e. the classes of the set $\bar{J} = \{j \in \{1,2,\dots,J\} : N_j^O > 0\}$. The modification of the j-th class consists in adding the N_j^0 of the enforcements to this equivalence class, and for each added enforcement of execution of the operation of the $\widehat{\oplus}$ upper bound operator on the enforcement and the upper bound of the class, to which this enforcement is attached. The time needed to implement the above is:

$$\tau_{KR} = \tau_R|\bar{J}| + \tau_o \sum_{j\epsilon\bar{J}} N_j^O = \tau_R|\bar{J}| + \tau_o N^O \quad (16)$$

and the efficiency of using the lattice model:

$$\varepsilon = \frac{\tau_R(I+N^O)}{\tau_R|\bar{J}|+\tau_o N^O} \quad (17)$$

The efficiency with the above method of taking into account new enforcements is lower than that presented in the first case (there is a larger number of classes considered $|\bar{J}| > 1$). The least effective case occurs when each added enforcement is the member of another class of equivalence ($|\bar{J}| = N^O$) of expanding the process to include new enforcements can be determined as ε_R:

$$\varepsilon_R = \frac{\tau_R(I+N^O)}{\tau_R|\bar{J}|+\tau_o N^O} = \frac{\tau_R(I+N^O)}{(\tau_R+\tau_o)N^O} \quad (18)$$

Therefore, the variation range of the efficiency coefficient may be presented as:

$$\frac{\tau_R(I+N^O)}{(\tau_R+\tau_o)N^O} \leq \varepsilon_R \leq \frac{\tau_R(I+N^O)}{\tau_R+\tau_o(N^O-1)} \quad (19)$$

In the case of expanding the task handling process, it takes place in practice and $I \gg N^O$ and $\tau_r \sim \tau_o$ which allows for the estimation to be adopted:

$$\varepsilon_R \sim 1 + \frac{I}{N^O} \quad (20)$$

which leads to the conclusion that the lattice mechanism allows for very effective preservation of access security and data flow under the conditions of development of processes for handling the system tasks.

4. Calculation example for the efficiency tested

In order to better illustrate the formulae in Chapter 3, the author has developed the calculation example. As the real time of performing specific functions or checks is not important, only the comparison of the efficiency of the mechanism with and without the lattice model. The currently standard 4 GHz processor clock is assumed (we are considering a simple case of single-threaded processing), which gives 0.25 ns per processor cycle. When analysing the operations required to perform the various tasks of the programme operation (in this case the security mechanism), it was possible to estimate the time taken to complete them. Since for the purposes of efficiency it is mainly the relationships between the times (and not the exact final time) that are crucial, the tasks have not been described in detail. Estimated times for specific tasks as well as the range of variables (their possible parameterisation) are set out below:

- I – the number (of occurrences) of enforcements in the existing process will be the variable from 1 to 400,
- J – the number of equivalence classes will depend on the number of enforcements – considered in three cases: (a) optimistic – 20% * I – high similarity, few equivalence classes which improves the process; (b) medium – 50% * I – medium similarity; (c) worst – 100% * I, each element being its own distinct equivalence class, total diversity).
- N – number of types / kinds of enforcements (used in the formula (10)), depending on the division into collections of equivalence classes, and their number. The same three cases as for J were assumed, i.e. (a) optimistic – 20% * I – high similarity, few equivalence classes; (b) medium – 50% * I – medium similarity; (c) worst – 100% * I, each element being its own distinct equivalence class, total diversity, each equivalence class containing one element).

- τ_u – time of creation of the collection of equivalence classes – an initial task which requires a review of the entire collection of inducements and the creation of appropriate equivalence collections. It can be assumed that this is a fixed preparation time (50 ns have been adopted), operations related to the review of each enforcement (I * 1 ns) and operations related to each equivalence class (J * 1 ns) – the following value has been assumed: 50 ns + I * 1 ns + J * 1 ns.
- τ_R – the time of performing one check for three relations ρ, τ and δ – it is the time necessary to perform a comparison and a series of functions with VF (described in detail in [5]) for each of the three relations separately (according to the author's analysis and assumptions $\tau_R \rangle \tau_o$) – the value of 20 ns was assumed.
- τ_o – time of one operation of the operator $\widehat{\oplus}$ on the elements of requests (a small task which requires an indication of the end of the lattice) – the value of 2 ns was adopted.

Using the formula (13) and the times adopted above, charts can be drawn for three cases of the examination for correctness of the process of handling the public task, comparing times with the usage of the general model and the lattice based model:

a) Optimistic (few large equivalence classes, high similarity of enforcements):

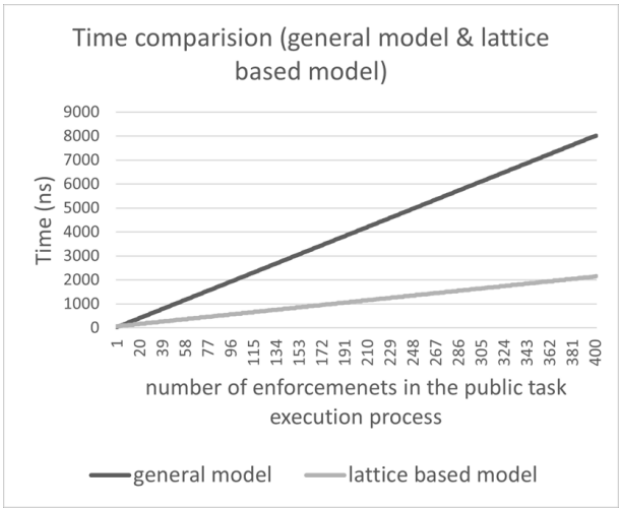

Fig. 1. The comparison of the times of the examination for correctness of the process of handling the public task with the usage of the general and lattice model (optimistic case)

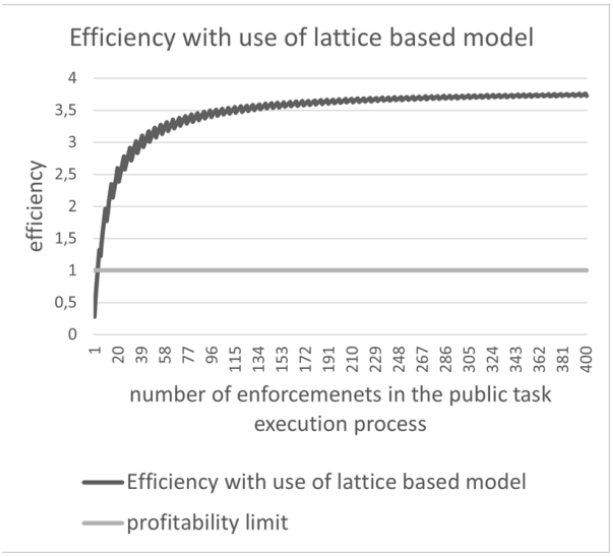

Fig. 2. The efficiency chart of examination time for correctness of the process of handling the public task with the usage of a lattice model (optimistic case)

As shown in Figures 1 and 2, after exceeding a certain small number of enforcements (in the above case 4) in the process of handling the public task and with the optimistic assumption of high similarity of enforcements, the coefficient of efficiency with the usage of the lattice model is higher than 1 and, with a large number of enforcements, it is stabilized at a high level (in the above case, the efficiency rate is 3.75).

b) average (50% similarity):

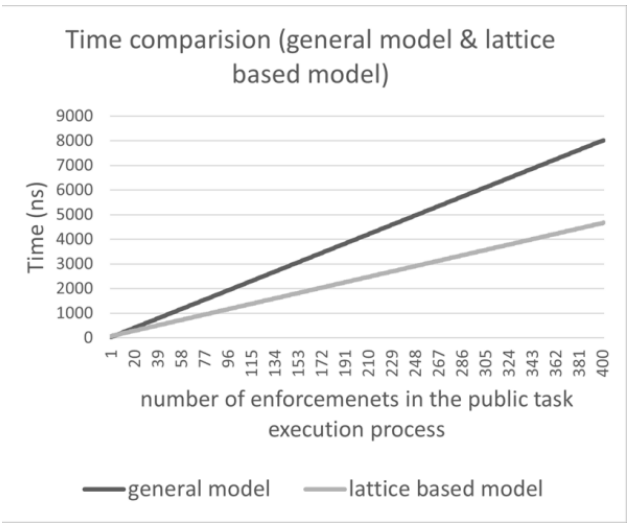

Fig. 3. The comparison of the times of the examination for correctness of the process of handling the public task with the usage of the general and lattice model (average case)

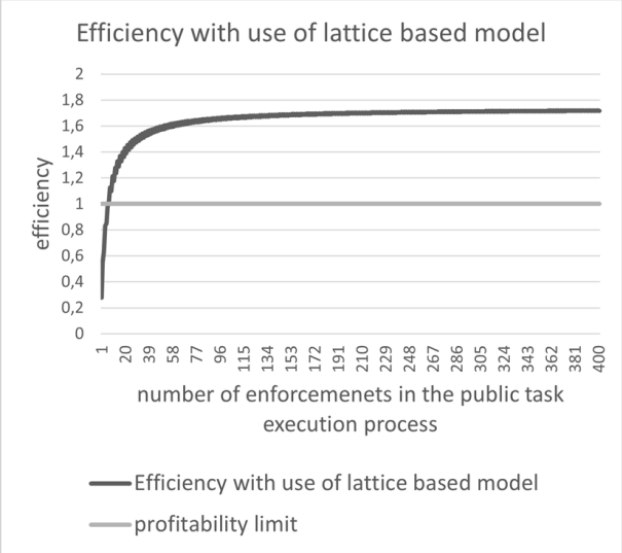

Fig. 4. The chart of the efficiency of the time of examination for the correctness of the process of handling the public task with the usage of a lattice model (average case)

As shown in Figures 3 and 4, after exceeding a certain small number of enforcements (in the above case 8) in the process of handling the public task and assuming the average similarity of enforcements, the coefficient of efficiency with the usage of the lattice model is higher than 1 and, with a large number of enforcements, it stabilises at a satisfactory level (in the above case, the efficiency rate is 1.7).

The average case analysed still shows the positive impact of the use of the lattice model on the level of time efficiency of the examination of the correctness of the process of handling the public task. The use of lattices and equivalence classes makes sense only from a certain minimum number of enforcements in the handling process (in the case of very short processes – few inducements – the use of lattices makes no sense as it adds an additional mark-up with a small profit).

c) worst (no similarity – each element in a separate equivalence class):

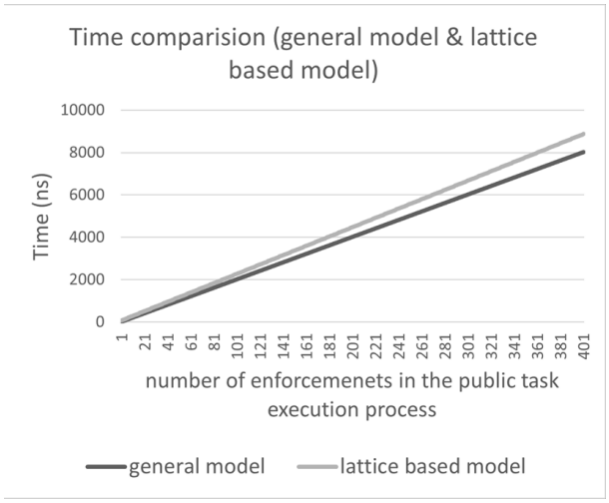

Fig. 5. The comparison of the times of the examination for correctness of the process of handling the public task with the usage of the general and lattice model (worst case)

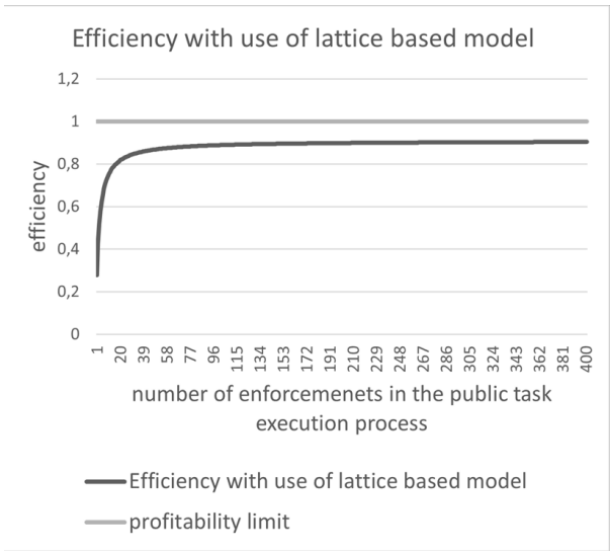

Fig. 6. The comparison of the times of the examination for correctness of the process of handling the public task with the usage of the general and lattice model (worst case)

In the worst case (i.e. lack of similarities of enforcements), as shown in Figures 5 and 6, the time efficiency of the examination for the correctness of the process of handling the public task with the usage of a lattice model is lower than in the case of the general model (regardless of the number of enforcements). In the case of total diversity, the usage of the lattice model and equivalence classes is an additional mark-up that does not generate any profit. Given that such a case of complete diversity is unlikely (it will occur as rarely as the best case) it is not a reason to reject a solution using the lattice model.

Using predetermined times and formula (19), it is also possible to indicate the range of

the efficiency coefficient for the expansion of the public service handling process by additional enforcements (for this example it is assumed that the number of additional new enforcements will be $N^O = 10$).

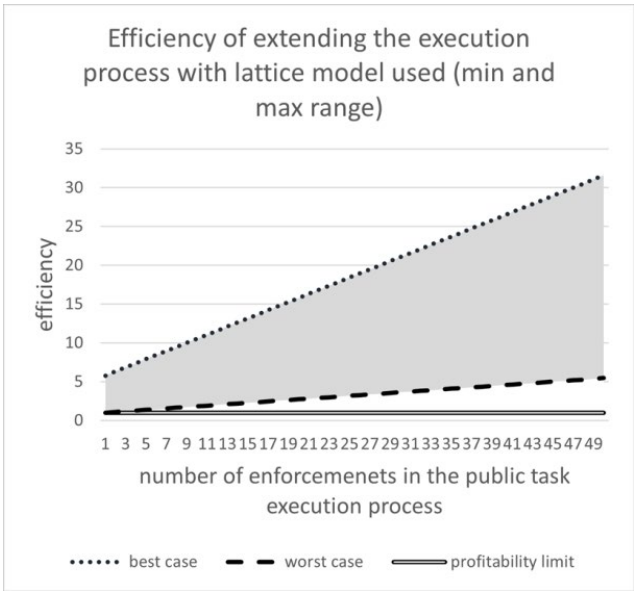

Fig. 7. The comparison of the times of the examination for correctness of the process of handling the public task with the usage of the general and lattice model

Figure 7 confirms the relation expressed by equation (20), indicating that the efficiency of the expansion of the handling process built with the usage of the lattice model (the area marked in the graph) is greater than one and increases as the difference between the already defined enforcements and the added enforcements increases ($I \gg N^O$). The greater the similarity of the added enforcements (fitting into already existing equivalence classes), the greater the efficiency coefficient (dotted line – best case). The worst case (largest variety of new added inducements) with the usage of the lattice model, still provides an efficiency of more than 1 (dashed line).

5. Summary and conclusions

Both the theoretical calculations and the presented calculation example confirm that the usage of lattices and equivalence collections provides better time efficiency in relation to the general model both in case of the examination of the correctness of the process of handling the public task and in case of the expansion of the process of handling the public task. Only in extreme cases of examination of correctness (from a security point of view) will this time efficiency be less than one (small string of enforcements, full diversity), as the effort associated with the introduction of the lattice model and equivalence collections will not generate the expected profits. As indicated in the paper such negative extreme cases are unlikely and at the same time can be offset by the extreme values from the best case.

The developed computational examples were made on the basis of the author's analysis of the practical execution (implementation) of the model presented in Chapter 2 (in pseudo-code – the paper under development). Another research task in developing the proposed model is its practical implementation in the selected programming language (based on mathematical [5] and architectural[1] model developed by author).

6. Bibliography

[1] Bliźniuk G., Szafrański B., *Interoperability and security of public administration information systems*, PTI, Katowice 2006.

[2] Denning D.E., Denning P.J., *Certification of Programs for Secure Information Flow*, Department of Computer Science Technical Reports, Purdue University, 1976.

[3] Górski T. (Ed.), *Platformy integracyjne: zagadnienia wybrane* (*Integration platforms – selected issues*), PWN, Warszawa 2012.

[4] Szafrański B., *Modelowanie procesów bezpieczeństwa baz danych ze szczególnym uwzględnieniem ich integracji* (*Databases security processes modelling, with particular emphasis on their integration*), Military University of Technology, Warszawa 1987.

[5] Szafrański B., Wilk J., "Mathematical modelling of processes to handle public tasks in the electronic platform environment", in: *Proceedings of the 36th International Business Information Management Association Conference* (IBIMA), 4–5 November 2020, Granada, Spain, 10236–10248.

[6] Wilk J., Szafrański B., "Electronic services security management for the public administration", *Computer Science and Mathematical Modelling*, No. 4, 25−32 (2016).

[1] Article on the architectural model and implementation of the solution in the cloud environment accepted for publication in 38th IBIMA International Conference proceedings.

[7] Wilk J., "Security of Composite Electronic Services"*, International Journal of New Computer Architectures and their Applications* (IJNCAA), Vol. 5, No. 3, 127–140 (2015).
[8] Wilk J., "The use of lattice theory in the modelling of safety management processes in public administration electronic services platforms" („Wykorzystanie teorii krat w modelowaniu procesów zarządzania bezpieczeństwem w platformach usług elektronicznych administracji publicznej"), *Roczniki Kolegium Analiz Ekonomicznych*, No. 33, 581–597 (2014).

Efektywność kratowych mechanizmów bezpieczeństwa wspierających obsługę zadań publicznych na cyfrowych platformach integracyjnych

J. WILK

Platformy integracyjne są rozwiązaniem coraz częściej wykorzystywanym przez administrację publiczną w Polsce w celu udostępniania i realizacji (w formie usług elektronicznych) na nich zadań publicznych. Autor we wcześniejszych publikacjach zaproponował matematyczny model bazujący na mechanizmach kratowych, który zapewnia bezpieczną realizację tych usług (z perspektywy ochrony poufności). W tej publikacji autorski model został przytoczony (jego główne elementy), a następnie wykonano analizę efektywności czasowej podejścia z wykorzystaniem mechanizmów kratowych z modelem ogólnym. Badana efektywność dotyczyła zarówno realizacji zadań publicznych – a dokładniej weryfikacji ich poprawności z perspektywy bezpieczeństwa przed realizacją, jak i rozszerzania procesu obsługi zadania publicznego. Autor wykazał, że w obu przypadkach stosowne jest wykorzystanie rozwiązania kratowego, ponieważ jego efektywność czasowa jest lepsza.

Słowa kluczowe: realizacja zadań publicznych, efektywność, model bezpieczeństwa, model kratowy.