High Granular Multi-Level-Security Model for Improved Usability

Dirk Thorleuchter
Fraunhofer INT
Euskirchen, Germany
dirk.thorleuchter@int.fraunhofer.de

Dirk Van den Poel
Faculty of Economics and Business Administration
Ghent University, Department of Marketing
Gent, Belgium
dirk.vandenpoel@ugent.be

***Abstract*— Working with existing multi-level-security (MLS) models reduces the usability especially when users try to transfer information to persons with different security categories. A main reason for the problems occurring with the information exchanging is that the existing MLS models assign a specific security level to documents. The assigned security level equals the highest security level of the textual content within the document. Based on the commonly used Bell LaPadula model, an extended model with an increased granularity is introduced. It is shown that users can access to parts of documents with higher security levels without causing a security compromise. This enables information exchange and it leads to an increased usability of the MLS model.**

Multi-level-security; Security; Modeling; Usability

I. INTRODUCTION

A well known problem with multi-level-security (MLS) models is that a workflow among users with different security levels could not be realized because of the 'write down' and 'read up' rules. It is not permitted for a user to write information in a document with lower security levels and it is also not permitted for a user to read in documents of higher security levels [10, 18]. Thus, a user with a lower security level could not read comments from a user with a higher security level. Additionally, the user with the higher security level could not write remarks in the document written by the user with a lower security level. A workflow between those two users is therefore not possible [7].

Existing MLS models based on a document granularity [13, 17]. Thus, the security level of a document equals the highest security level of the information stored in the document although there might be further information stored in the document that are of a lower security level. Considering the different kinds of security levels in a document could help to implement a workflow between the two users because then, selected information of the document can be exchanged without causing a security compromise.

Additionally, an increase granularity of information might increase the usability of a MLS model because several knowledge extraction and text mining approaches require a granular view on textual information [4, 19-26]. However, the existing MLS models do not consider an increased granularity view on the data [9, 11]. To realize an increased granularity, a new MLS model has to be build. The basic idea that stands behind this new approach is that information is not stored directly in a document but in objects of different security labels and that a document consists of a set of objects.

This work introduces a new approach for an MLS model that is based on an increased granularity view on the data. For this, it is important to provide background information first. Thus, in Sect. II a definition of a secure computer system is given and it is also explained how this system could be modeled (see Sect. III). Sect. IV presents the current Bell-LaPadula MLS model [1, 2]. Based on the information given in Sect. II-IV, a new MLS model is provided in Sect. V. An example for the use of the new MLS model and conclusions are given in Sect. VI and VII.

II. DEFINITION OF SECURE COMPUTER SYSTEMS

A computer system regardless weather it is secure or not consists of at least one operating system. Additionally, a computer system also could be defined as a network of single computer systems each consisting of at least one operating system. For an operating system, one can distinguish between two different operating modes: the mode system high and the mode MLS.

The operation mode system high means that all information is processed commonly regardless weather it consists of different security classifications. Further, the operation mode system high defines the security classification of the system in total as the highest classification of the information stored or processed in the system. Most current available operation systems (e.g. Windows, Linux, Unix) run in the operation mode system high.

In contrast to this, the operation mode MLS is defined by a completely separated processing of information based on their security classifications. This assumes specific software for the operation system but also for the data storage system etc.). Examples for operation systems run in operation mode MLS are Secure Version of MS Windows Vista, Secure Linux (Red Hat, Suse, Debian, Fedora), Trusted Solaris, SEVMS (Secure VMS), BAE Systems XTS-400, and CMW (Compartmented Mode Workstation) [16].

The existing MLS models standing behind the above mentioned operation systems focus on two aspects: the aspect of confidentiality and integrity of data [8] and the aspect of access control [12, 15]. In general, four different models can be seen. The Bell LaPadula model [5, 14] is a well-known, very often used model in the public sector. It

focuses on the confidentiality of data. This is in contrast to the Biba model [3] that leads to integrity of data in the public sector. The Clark-Wilson model is a well-known model in financial sector that based on integrity of data. A model in the financial sector that based on access control is the Brewer and Nash model.

This paper is based on the Bell LaPadula model as most commonly used in practice. This model consists of two kinds of security categories [15]: The classification category (in literature this category is often mentioned as security level) and the needs-to-know categories (in literature this category is often mentioned as compartmented information). A classification category consists of an hierarchical structure (e.g. top secret > secret > confidential > restricted > unrestricted). Examples for the needs-to-know categories are US Eyes only, Company Eyes only, atomic etc [6].

Thus, in this paper a secure computer system is defined as a computer system in operation mode MLS based on the Bell LaPadula model.

III. System Modeling

For modeling a computer system, the relations among objects have to be defined by providing a description of the computer system in a formal way. Three properties are important - the generality, the predictive ability, and the appropriateness / usefulness:

"A model too closely tied to a specific application loses the possibility of more general applicability. On the other hand, a model insufficiently rooted in the problem at hand will not allow accurate prediction of the behavior of the computer system being modeled … The last important feature of a model is its appropriateness to the situation of interest" [1].

A computer system as functional system in its most general form can be formulized as relation on three sets: S = X x Y x Z whereby the elements of X represent inputs, the elements of Y represent outputs, and the elements of Z represent internal system states. Thus, S is a function that transforms X, Z to Y, Z'.

IV. The Bell LaPadula MLS Model

Modeling a secure computer system means considering that a secure computer system has multiple users. Common data bases or files in the file system are used concurrently. The data units are assigned to one security level each and to several need-to-know categories. Additionally, each user also is assigned to a security levels and to several need-to-know categories. Thus, elements of a secure computer system are subjects and objects.

In Bell LaPadula model, elements of the model are defined as follows: S: $\{S_1, \ldots, S_n\}$ are the subjects that means processes and programs in execution. O: $\{O_1, \ldots, O_m\}$ are the objects that means data, files, and programs not in execution. C: $\{C_1, \ldots, C_q\}$ are the classifications, which means the clearance level of a subject and the classification of an object. The order of the classification is determined by $\{C_1 > C_2 > \ldots > C_q\}$. K: $\{K_1, \ldots, K_r\}$ are the needs-to-know categories that means projects, numbers, and access privileges. Further, PK is defined as the power set of K.

Each Subject S has both, a classification and a need-to-know property.

$$(C^S , PK^S). \quad (1)$$

Further, each Object O also consists of a classification and a need-to-know property.

$$(C^O , PK^O). \quad (2)$$

The 'no read up' rule says that reading of objects is allowed if and only if

$$C^S \geq C^O. \quad (3)$$

and

$$PK^O \subseteq PK^S. \quad (4)$$

The 'no write down' rule says that writing of objects is allowed if and only if

$$C^O \geq C^S. \quad (5)$$

and

$$PK^S \subseteq PK^O. \quad (6)$$

The case of $C^O > C^S$ or $PK^S \subset PK^O$ is named blind writing because a subject is not allowed to read in an document that is of a higher classification or of different needs-to-know categories. However, the subject is allowed to write in this object.

V. The Proposed MLS Model

Here, we present a new MLS model based on the Bell LaPadula model as described in Sect. IV. This new approach extends the Bell LaPadula model to a more granularity view on data. This is done by presenting a formal description. In Sect. VI, an example for common processing of different sensitive information using this new approach is presented.

In Definition 1, we formulize a frame object that consists of several objects with different security levels and different sets of needs-to-know categories. In contrast to Bell LaPadua model, a frame object is not restricted to one security level and to one set of needs-to-know categories. Therefore, with frame objects, we can create e.g. texts that contain information from different security levels. This is not possible in the standard Bell LaPadula model where a text in total is assigned to the highest security level of its objects.

Definition 1: Let an object $O\{i,j\}$ be data, files, programs, subjects etc. as defined in Bell LaPadula model. Let a frame object O^{sup}_i be a list of objects. Let $n \in N$ be the number of frame objects in a multi level security system and $i \in \{1,..,n\}$. Let $m_i \in N$ be the number of objects in O^{sup}_i and $j \in \{1,.., m_i\}$. Then a frame object is fomulized as

$$O^{sup}_i \equiv [O\{i,1\}, .., O\{i,m_i\}]. \quad (7)$$

In Definition 2, we describe the classification and need-to-know properties of objects and - in contrast to Bell LaPadula model – we describe that a frame object does not consist of a classification and a need-to-know property.

Definition 2: Let C be a classification category (security level). Let $C^{O\{i,j\}}$ be the classification category of an object as defined in Bell LaPadula model. Let K be the compartment information. Let P be the power set. Let $PK^{O\{i,j\}}$ be the needs-to-know categories of an object that means the power set of all object specific compartment information as defined in Bell LaPadula model. Then, object categories are formulized as

$$(C^{O\{i,j\}}, PK^{O\{i,j\}}). \quad (8)$$

The categories for all frame objects are defined as empty set.

$$C\{ O^{sup}_i \} == \varnothing. \quad (9)$$

$$PK\{ O^{sup}_i \} == \varnothing. \quad (10)$$

In Definition 3 the 'no read up' rule is described. It is adopted from the Bell LaPadula approach and extended by considering the definitions in the new MLS model.

Definition 3: Let a subject S{k} be a process, programs in execution etc. as defined in Bell LaPadula model with subject categories ($C^{S\{k\}}$, $PK^{S\{k\}}$). Let $p \in N$ be the number of subjects in a multi level security system and $k \in \{1, ..., p\}$. Let reading of object O{i,j} by subject S{k} be allowed if and only if

$$C^{S\{k\}} \geq C^{O\{i,j\}}. \quad (11)$$

and

$$PK^{O\{i,j\}} \subseteq PK^{S\{k\}}. \quad (12)$$

Definition 4 does not lean on the 'no write down rule' from the Bell LaPadua approach. Here, we create a new object and write in this object. This is because to allow a user to write data in frame objects that consists of several objects with different security levels and different sets of needs-to-know categories. This does not cause a security compromise.

Definition 4: Let an object

$$O\{i,j\} \equiv [data\{i,j,1\}, .., data\{i,j,q_{i,j}\}] . \quad (13)$$

be a list of data units e.g. picture, document, paragraph, line, sentence, text phrase, word, syllable, sign etc. Let $q_{i,j} \in N$ be the number of data units in an object O{i,j}. Let $l \in \{1, .., q_{i,j}\}$ be the position where a subject S{k} insert content. Let a writing split $O_w\{i,j,l\}$ on the position l of an object O{i,j} be a list of three objects.

$$O_w\{i,j,l\} \equiv [O\{i,j,1\}, O\{i,j,2\}, O\{i,j,3\}]. \quad (14)$$

with

$$O\{i,j,1\} \equiv [data\{i,j,1\}, ..., data\_\{i,j,l-1\}]. \quad (15)$$

and

$$O\{i,j,3\} \equiv [data\{i,j,l\}, \ldots, data\{i,j,q_{i,j}\}]. \quad (16)$$

Let $O\{i,j,2\} \equiv \varnothing$ be a new and empty object. Let writing in object O{i,j,2} – and thus, in O{i,j} - by subject S{k} be allowed if and only if $C^{O\{i,j,1\}}$, $C^{O\{i,j,2\}}$, $C^{O\{i,j,3\}}$, $PK^{O\{i,j,1\}}$, $PK^{O\{i,j,2\}}$, $PK^{O\{i,j,3\}}$, and O^{sup}_i are defined as follows:

$$C^{O\{i,j,1\}} \equiv C^{O\{i,j,3\}} \equiv C^{O\{i,j\}}. \quad (17)$$

and

$$PK^{O\{i,j,1\}} \equiv PK^{O\{i,j,3\}} \equiv PK^{O\{i,j\}}. \quad (18)$$

and

$$C^{O\{i,j,2\}} \equiv C^{S\{k\}}. \quad (19)$$

and

$$PK^{O\{i,j,2\}} \equiv PK^{S\{k\}}. \quad (20)$$

and

$$O^{sup}_i \equiv [O\{i,1\}, \ldots, O_w\{i,j,l\} , \ldots, O\{i,m_i\}]. \quad (21)$$

In Definition 1 a frame object is defined. Based on Definition 2, a subject can access the frame object O^{sup}_i without causing a security compromise because its categories are defined as empty set. Further, the subject is allowed to read in selected objects from the frame object as defined by Definition 3. The subject also can write in the newly created object O{i,j,2} according to Definition 4. Thus, this is allowed for reading and writing in a frame object O^{sup}_i regardless wether the frame object contains information with a higher security level.

In the next section, an example is presented for using the new MLS model.

VI. RESULTS AND DISCUSSION

Using these new definitions lead directly to a more granularity view on data. Therefore, we present a simple example for common processing of different sensitive information using this new approach. People from strategic management add information that is classified as "enterprise confidential" to a text that is unclassified (see Fig. 1).

By use of the Bell LaPadula MLS model the text is classified as "enterprise confidential" in total. This means, the first sentence is automatically assigned an "enterprise confidential" security label.

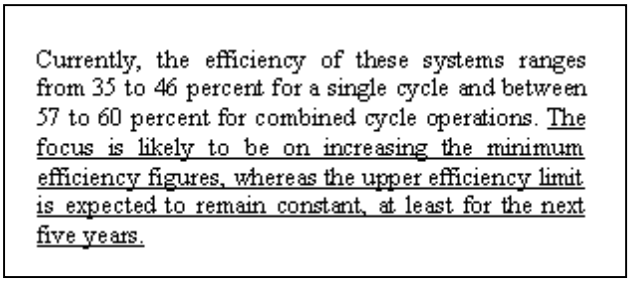

Figure 1. A text with an unclassified first sentence and a "enterprise confidential" classified second sentence (underlined).

Some interesting effects occur, e.g. the author of the first sentence – we assume that the author is not permitted to access "enterprise confidential" documents – is not allowed to read his own sentence. Further, all company professionals that do not have an appropriate clearance are also not able to access to this modified document.

By use of the new MLS model introduced here, it is possible that these professionals access the document by viewing the first sentence only. This is because the document itself is not "enterprise confidential" but only the second sentence.

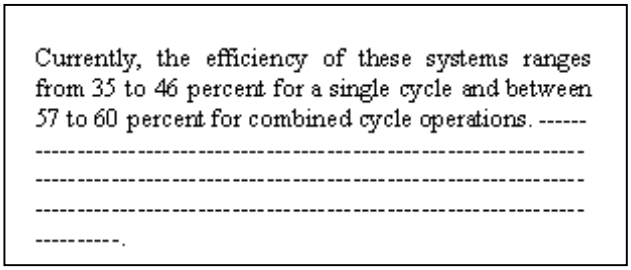

Figure 2. With the new MLS model, professionals are allowed to access the doument and view the first sentence even if they are not allowed to access "enterprise confidential" documents.

VII. Conclusions

This paper provides a new MLS model with increased granularity. For this, the existing Bell LaPadula model is extended. A disadvantage of the Bell LaPadula model is that the security classification of a document equals the highest security classification of its content. This leads to problems in the usability. The newly introduced MLS model bridges this gap. This leads directly to an increased usability.

References

[1] D.E. Bell and L. J. LaPadula, "Secure Computer Systems: Mathematical Foundations," Bedford: Mitre Corp., 1973.

[2] D. E. Bell and L. J. LaPadula, "Secure Computer System: Unified Exposition and Multics Interpretation," Bedford: MITRE Corp., 1976.

[3] K. J. Biba, "Integrity Considerations for Secure Computer Systems," Bedford: Mitre Corp., 1977.

[4] J. Burez and D. Van den Poel, "Handling class imbalance in customer churn prediction," Expert Systems with Applications, vol 36 (3/1), pp. 4626-4636, 2009.

[5] S. Chokhani, "Trusted products evaluation," Commun ACM, vol. 35 (7), pp. 64-76, 1992.

[6] R. J. Feiertag, K. N. Levitt, L. Robinson, "Providing multilevel security of a system design," Proc. 6th ACM Symp. Operating System Principles, 1977.

[7] W. Gericke, D. Thorleuchter, G. Weck, F. Reilaender, and D. Loss, "Vertrauliche Verarbeitung staatlich eingestufter Information - die Informationstechnologie im Geheimschutz," Informatik Spektrum, vol. 32 (2), pp. 102-109, 2009.

[8] J. Herranza, S. Matwin, J. Nind, V. Torra, "Classifying data from protected statistical datasets," Comput Secur, vol. 29 (8), pp. 875-890, 2010.

[9] S. Holeman, G. Manimaron, J. Davis, A. Chakrabarti, "Differentally secure multicasting and its implementation methods," Computer Security, vol. 21 (8), pp. 736-749, 2002.

[10] M. D. Hunter, "An Information Security Handbook," Berlin: Springer, p. 5, 2001.

[11] C. E. Landwehr, "Formal models for computer security," Comput Surv, vol 13 (3), 1981.

[12] E. Y. Li, T. C. Du, J. W. Wong, „Access control in collaborative commerce," Decis Support Syst, vol. 43, pp. 675-685, 2007.

[13] R. Lindgreen, I. S. Herschberg, "On the validity of the Bell-LaPadula model," Comput Secur, vol. 13, pp. 317-333, 1994.

[14] J. McLean, "A comment on the Basic Security Theorem of Bell and LaPadula," Inf Process Lett, vol. 20, 1985.

[15] S. Obiedkov, D. G. Kourie, J. H. P. Erloff, „Buildung access control models with attribute exploration," Comput Secur, vol. 28, pp. 2-7, 2009.

[16] P. Pfleeger, S. L. Pfleeger, "Security in computing," Old Tappan: Prentice Hall, 2003.

[17] J. H. Saltzer, M. D. Schroeder, "The protection of information in computer systems," Proc IEEE 1975; 63(9):1278-1308.

[18] R. Slade, "Dictionary of Information Security," Burlington: Syngress; 2006, p. 125.

[19] D. Thorleuchter., D. Van den Poel, "Companies Website Optimising concerning Consumer's searching for new Products," in: Proc. URKE 2011, IEEE Press, 2011, ISBN: 1424499852.

[20] D. Thorleuchter, "Finding new technological ideas and inventions with text mining and technique philosophy" in: Data analysis, machine learning and applications, C. Preisach Ed. Berlin: Springer, pp. 413-420, 2008.

[21] D. Thorleuchter, D. Van den Poel, and A. Prinzie, "A compared R&D-based and patent-based cross impact analysis for identifying relationships between technologies," Technological Forecasting and Social Change, vol 77 (7), pp. 1037-1050, 2010.

[22] D. Thorleuchter, D. Van den Poel, and A. Prinzie, "Mining Ideas from Textual Information," Expert Systems with Applications, vol. 37 (10), pp. 7182-7188, 2010.

[23] D. Thorleuchter, D. Van den Poel, and A. Prinzie, "Extracting Consumers Needs for New Products," in Proceedings of WKDD 2010, IEEE Computer Society, CA: Los Alamitos, pp. 440-443, 2010.

[24] D. Thorleuchter, D. Van den Poel, and A. Prinzie, "Mining Innovative Ideas to Support new Product Research and Development," in Classification as a Tool for Research, H. Locarek-Junge and C. Weihs Eds. Berlin: Springer, pp. 587-594, 2010.

[25] D. Thorleuchter, D. Van den Poel, and A. Prinzie, "Analyzing existing customers' websites to improve the customer acquisition process as well as the profitability prediction in B-to-B marketing, " Expert Systems with Applications, to appear, doi: 10.1016/j.eswa.2011.08.115.

[26] D. Thorleuchter and D. Van den Poel, "Semantic Technology Classification - A Defence and Security Case Study," Proc. URKE 2011, IEEE Press, 2011, ISBN: 1424499852.