MULTI-LEVEL SECURITY CANNOT REALISE NEC OBJECTIVES

Harm Schotanus M.Sc, Tim Hartog M.Sc, Cor Verkoelen B.Sc
Information Security Dept., TNO Information and Communication Technology, Delft, The Netherlands
Harm.schotanus@tno.nl
Tim.hartog@tno.nl
Cor.verkoelen@tno.nl

Abstract:
Multi-Level Security (MLS) is often viewed as the holy grail of information security, especially in those environments where information of different classifications is being processed. In this paper we argue that MLS cannot facilitate the right balance between need-to-protect and duty-to-share as required for a Network Enabled Capability (NEC) based military operations. This is due to the fact that MLS is deemed rigid in its restrictions; it obstructs the flow of information towards lower classifications by definition and thus influences duty-to-share; furthermore MLS results in a set of rigid preconditions for the physical environment to guarantee the required need-to-protect. The focus of a security solution instead should be on flexibility towards information sharing and reducing risks to be useful in a NEC environment. This can be achieved by firstly reducing the size (and complexity) of the systems that contain the classified information systems, using Multiple Independent Levels of Security (MILS) to create these smaller, separated compartments; and secondly controlling the information flow between the (different) classified compartments by dynamic policies. Moreover, the realignment of classification provisions can make management of information much more flexible and efficient. Hence, we can finally forget MLS.

Keywords: MLS, MILS, information security, classified information, policies.

1 Introduction

Ever since the 1970s Multi-Level Security (MLS), defined by the National Security Institute (1985), is often viewed as the holy grail of information security for working with information of different classifications. Despite these high expectations, it has never become reality on a large scale and most of the time a system-high approach is taken instead. MLS is still an idea for the future. Despite that MLS is mainly concerned about regulating access to classified information and the actions that are allowed, it is often expected that MLS will be able to solve any security problem with regard to classified information.

The question nevertheless is whether MLS would solve the actual problems at hand. In other words, can MLS find the right balance between need-to-protect and duty-to-share that is required for realizing the Network Enabled Capability (NEC)?.

2 Objectives of Military Information Systems

Military operations are increasingly carried out with partners from different nations and in partnership with non-military organisations in order to reach the operational objectives. Current military communication infrastructures are deployed as stand-alone networked information systems operating in the system-high mode. However, effective and efficient cooperation among the different coalition partners requires information sharing – with the motto “the right information at the right place at the right time” (Buckman 2010). It is not acceptable in many cases to outright share all information among all partners. Hence, it is necessary to be able to determine which information is suitable for sharing with other partners, and enforcing these decisions.

MLS is often positioned to solve the problem of “the right information at the right place at the right time”, without unnecessarily violating information security rules. The main question is whether that is correct. In this paper we attempt to debase the unrealistically high expectations on MLS and provide alternative focal areas. We argue that MLS will not provide the right balance between need-to-protect and duty-to-share and we recommend that the development of military information systems focuses on alternatives to realise this goal.

These alternatives should provide flexibility towards implementing security restrictions and permissions. Rigid rules regarding the treatment of classified information, as is the case in MLS, inhibits the sharing of information as they only define limitations but do not capture the need-to-share principle. The need-to-share principle implies that the mandate for information sharing decision

making is delegated to the authorised users of the information. Thereby increasing the risks involved proportionally to the amount of information accessible to a user. It is therefore fundamental to reduce risk without impeding the capability to share information.

3 Multi-Level Security

3.1 Origin

MLS has been created to enforce access control in military and government information systems, especially aiming at the separation of information of different classifications within a single system. This implies a focus on confidentiality protection. To provide this protection, the MLS concept was created, for which the primitives are formulated in the Bell-LaPadula Model by Bell and La Padula (1973). The BIBA model by Biba (1977) is an alternative MLS model. However in most military domains, confidentiality is still the primary concern, whereas BIBA primarily addresses integrity.

The Bell-LaPadula access control model states that based on the user's clearance and their need-to-know the user may access a subset of the classified information within the system. Access is defined by two rules of mandatory access control (MAC), as shown in Figure 1:

1. No read up (NRU) – no read access is permitted to an object with a higher classification than the clearance of the user.
2. No write down (NWD) – no write access is permitted to an object with a lower classification than the clearance of the user.

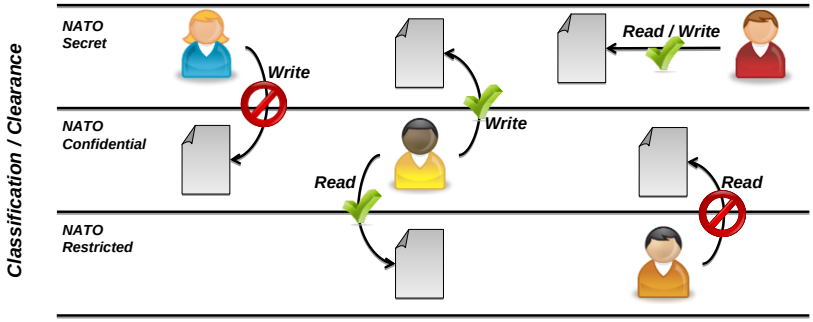

Figure 1. Access rules within Bell-LaPadula.

This ascertains that information cannot leak to users that do not have the proper clearance for that information and therefore fulfils the 'duty-to-protect' requirement.

3.2 Consequences

Fahs (2004), Bell (2005), Schaefer (2004) and Levin (2007) state that the application of the MLS model has a number of significant drawbacks with respect to the military information system objectives, aside from its technical feasibility. First, information can only flow upwards by definition – i.e. information with a certain classification can only be accessed by users with a higher or equal clearance. MLS does not provide any means for a user to share information with another user having a clearance that is lower than the information requires. All access control in a MLS system is only restrictive, and not permissive. The two MAC rules cannot be extenuated by a user, but only reinforced by discretionary access rules (DAC). The classification is always leading. This is in direct conflict with the objective of actually sharing information, need-to-share, as in many cases information is shared with users having a different or lower clearance. E.g. NATO Secret cannot be shared with NATO personnel with a NATO Confidential clearance, as the clearance does not permit this.

Second, whether information can be processed is not merely dependent on the clearance of the user and the classification of the information, but also depends on the environment in which the information is accessed. E.g. in an office cleared to process NATO Confidential information, an MLS terminal can be placed. Subsequently, a user with a NATO Secret clearance should be able to access NATO Secret information on the terminal assuming the user has a need-to-know. However, this would not be permitted because the environment is only cleared to process NATO Confidential information. The terminal is typically not capable of determining its location, and the security properties of this location.

This means that the highest classification of information that can be processed is determined by a combination of the clearance of the user and the physical location of the MLS terminal. Consequently the user cannot always access all the information for which he is cleared. Hence, this means that the configuration of an MLS system should address the physical location security properties and thereby making the configuration very static and inflexible. This inflexibility inhibits the possibility to access important information when it is needed and thus is in contradiction with the “right information at the right place, at the right time” as needed for an effective and efficient cooperation among the different coalition partners.

In addition the result of MLS is one system where all types of information can be processed and any user satisfying the access control requirements can access the system. However creating such a large system also increases the risk associated with processing classified information. This means that any possible flaw – technical or procedural – can escalate quickly into serious incidents. In such a large, and complex system as this, flaws are nearly a certainty.

In other words, an MLS solution is a very restrictive and inflexible model that enforces a single, rigid policy. It also inhibits any option for a user to make an alternative decision regarding the access to information or sharing of information. Access control and possible information sharing is determined by the MLS model itself, intelligent decisions made by a user are in direct conflict with the MLS concept. Hence it can be concluded that MLS does not facilitate sharing of information but instead will actually hinder it.

4 Alternatives to MLS

We need an alternative to MLS that provides a better balance between information sharing and information protection. This implies a shift in focus on solely protecting the confidentiality of the information to incorporate the assurance of the availability of the information. All the aspects that need to be addressed are briefly described in the following paragraphs. This includes technical components but also requires a change of attitude.

4.1 Classification management

An important aspect of working with classified information, is actually properly classifying the information. In traditional system high environments the incentive is to classify anything in the environment to the highest possible level, as stated by Neugent (2005). E.g. information in a NATO Secret domain is by default and implicitly classified as NATO secret. As a result the information pyramid is top-heavy as shown in Figure 2. In an optimal situation, most information will be classified as low as possible. Only a small amount information will have a high classification. In system high and MLS solutions the opposite is much closer to the truth. E.g. for a map with coordinates of artillery the map is not classified, but only the coordinates are. In a system high or MLS environment the whole map is classified.

As a result, the required security measures to protect all the information are costly, redundant and impede sharing information – the higher the classifications are, the more difficult it is to share. The value of classifying information is eroded. The noise of all the over-classified data will result in an increase of the risks by the incapability to distinguish the actual value of the information.

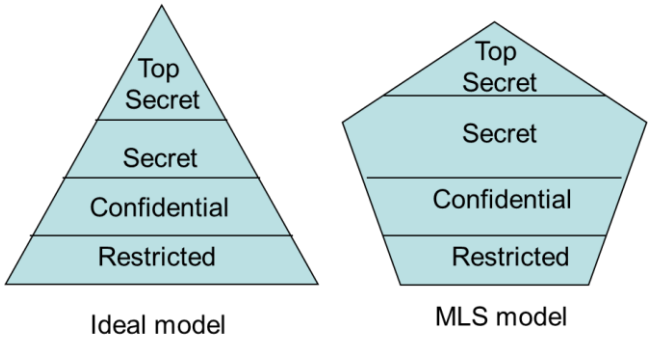

Figure 2. Information amounts per classifaction

Therefore in an environment such as envisioned by Buckman (1973) and proposed in by Hartog (2011) it is necessary to realign the way information is classified, with two important characteristics:

1. Information is classified as low as possible – implying that only that part of the information is classified that can be justified as such. E.g. for a map with coordinates of artillery, only these coordinates are classified and not the entire map.
2. Information is only classified for as long as the classification is actually needed and declassified when the classification is no longer reasonable.

The information system should provide the user the means to de- or reclassify information and as such make it easier to share information. However, in any case the user must be made responsible for all such actions.

4.2 Compartmentalization of information

Multiple Independent Levels of Security (MILS) is often cited as an alternative to MLS by Rushby (1981). Although the acronym is quite similar, the model is different. The MILS concept creates different information compartments on one system or computer, as shown in Figure 3. Each compartment can be used e.g. for a different classification. Vanfleet (2005) states that a so-called separation kernel ensures that information cannot flow between different classified compartments. And because each compartment behaves like an independent system, access control to, authorisation within these compartments can be specific for each compartment.

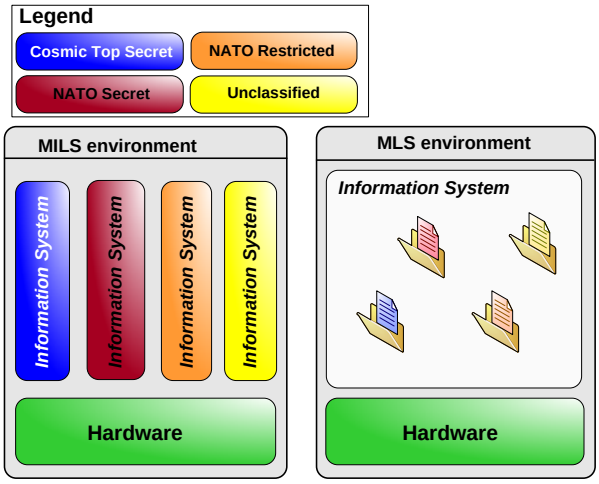

Figure 3. MILS versus MLS

In case a user needs access to information in a certain compartment it is his own decision to access that compartment given in which environment he is. In an MLS system this decision cannot be made by a user because the relation between information and the location is rigidly defined in the configuration of the MLS system.

4.3 Reduction of information per system

Processing classified information is always associated with residual risks that cannot be mitigated fully. The more information a system contains and the more users have access to that system, the higher these risks are. Hence, less information in a compartment means that the risks can be mitigated and managed better. As the amount of information needed by a user will not decrease as a whole, this implies that the compartments must be made smaller¸ but users may have to access more compartments. Because the residual risks are smaller, it is more acceptable for the organisation to delegate the responsibility to the user to make intelligent decisions about information sharing.

To reduce the size of the systems into smaller compartments and to support the decision making by a user, we must disentangle the infrastructure and the information and shift the security of the information towards the individual computer systems or eventually application as stated by Verkoelen (2010) and Hallingstad (2007)(2008). Having several compartments available for different types of information allows the reduction of the amount of information in each compartment.

4.4 Controlled information exchange

The information exchange between compartments of different classifications should not take place unrestrictedly. Hence, we need mechanisms to establish the controlled information exchange based on

user decisions. The mechanisms should reflect the agreements regarding the conditions of information sharing.

The design of a plane of interconnection between different compartments can be very complex. The elements of trust and threats should be leading in the design. Thereby the security functionality and policies are geared to the actual situation instead of forming rigid default configurations. Schotanus (2011) and Boonstra (2011) describe a methodology to analyse interconnections based on the trust assumptions and applicable threats for these interconnections. The methodology determines the security requirements and associated assurance levels.

The focus should be on creating standardised modules to realise a plane of interconnection that can provide means to control the information exchange between different compartments. The methodology can be used to select the modules for a specific situation.

4.5 Policies

The fixed security policies that many current systems and the MLS concept have, incur the inflexibility of the system. This inflexibility impedes the capability to have the user in control of which information can be shared within all the rules and agreements associated with modern military operations. To provide a flexible model for security, the applicable security policies should be separated from the security systems and enforced by the security mechanisms. The policy can be aligned with the present risks. This enables the adjustment of policies when needed, and the enforcement by security systems of the correct policies.

A security policy describes a set of rules that determines how the information must be processed in order to ensure the protection of the information sufficiently. We need a methodology to translate the abstract rules as defined in agreements into policies that can be enforced by the security mechanisms. The methodology should ensure the completeness and consistency of the applicable rules. Neugent (2005) states that the security mechanisms should be aligned with the present risks and that we need means to manage the security policies.

The rules should reflect a user action or in some cases an automatic action that has been applied to the information. Based on the act it is determined whether the permission to share the information can be granted. A crucial part of a policy is the accountability and therefore we need to register the information flow. An example of an act can be secure labelling of information as described by Oudkerk (2010), Hartog (2011) and Eggen (2010).

5 Conclusions

We have argued that MLS - the oft-cited all-in solution for processing classified information - cannot facilitate efficient sharing of a subset of information while guaranteeing the security requirements on the entire set of information. The reasons behind this are that in an MLS system information can flow only towards higher classifications and for information sharing, we actually need to facilitate the controlled flow of information to lower classifications. MLS cannot take the environment into account hence it has to on a static configuration whereas contrariwise flexibility is needed. Furthermore MLS moulds a huge system of all information which will only increase the risk in case of flaws, and for information sharing we actually need to reduce risks of flaws. MLS is a very strict and static model that enforces a fixed policy.

Hence it is necessary to shift the focus to other solutions instead of clinging to an unrealistic and essentially undesirable concept such as MLS. We have identified five elements that should be integrated into system designs. These are:

1. Improvement of classification management to reduce the amount of information that is classified and reduce the time information is classified.
2. Compartmentalisation of information by separating information of different classifications using Multiple Independent Levels of Security.
3. Reduction of the amount of information per compartment to limit the risk of flaws.
4. Controlled information exchange by using control mechanisms between different compartments based on user decisions.

5. Policy management to translate and manage abstract rules and agreements to machine interpretable rule sets that can be implemented in control mechanisms that validate user actions against a policy to facilitate the sharing of information between different compartments.

In this manner we can actually realise the objectives stated by the Network Enabled Capability. This primarily reflects the need for flexibility towards determining what information can be shared and with whom. However the need-to-share principal needs to be properly balanced by the need-to-protect. It is necessary to reduce the risk of information sharing that can be attained by dividing the information in smaller separate compartments. In addition, for disentangling the information and infrastructure, it is necessary to relinquish the implementation of security in the infrastructure and work towards applying policies on information flows. And then the concept of MLS can finally be shelved indefinitely.

REFERENCES

Bell, D.E. (2005) "Looking Back at the Bell-La Padula Model," *Proceedings of the 21st Annual Computer Security Applications Conference* (ACSAC), pp 337–351, 2005.

Biba, K.J. (1977) "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, http://seclab.cs.ucdavis.edu/projects/history/papers/biba75.pdf, April 1977.

Boonstra, D. and Schotanus, H.A. and Verkoelen, C.A.A. (2011) “A Methodology for the Structured Security Analysis of Interconnections”, http://ieeexplore.ieee.org/iel5/6111660/6127424/06127476.pdf, Milcom 2011

Buckman, T. (2010) “Nato Network Enabled Capability Feasibility Study – Executive Summary”, version 2.0, NC3A

Eggen, A., et al. (2010) “Binding of Metadata to Data Objects – a proposal for a NATO specification”, Norwegian Defence Research Establishment (FFI) & NC3A

Eggen, A., et al. (2010) “XML Confidentiality Label Syntax – a proposal for a NATO specification”, Norwegian Defence Research Establishment (FFI) & NC3A, 22 april 2010.

Fahs, R and Wiseman, S.R. (2004) “Re-Floating the Titanic: Multi Level Security in Contemporary Environments” Defence Research Agency. March. 2004.

Hallingstad, G. and Oudkerk, S. (2007) “Protected Core Networking – Initial concept description”

Hallingstad, G. and Oudkerk, S. (2008) “Selected aspects of Protected Core Networking”

Hartog, T., et al. (2011) “Labelling: Security in Information Management and Sharing” 6th International Conference on Information Warfare and Security

La Padula, L.J. and Bell, D.E. (1973) “Secure Computer Systems: A Mathematical Model,” MTR–2547, Vol. II, The MITRE Corporation, Bedford, MA,31 May 1973. (ESD–TR–73–278–II)

Levin, T.E., et al. (2007) Analysis of three multilevel security architectures; Proceedings Of Computer Security Architecture Workshop.

National Security Institute (1985) “5200.28-STD Trusted Computer System Evaluation Criteria”, http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt, December 1985.

Neugent, W., (2005) “Assured Information Sharing,” The Edge, The MITRE Corporation, Fall 2005

Oudkerk, S., et al. (2010) “A proposal for an XML Confidentiality Label Syntax and Binding of Metadata to Data Objects”, IST 091, 2010.

Rushby, J. (1981) “Design and Verification of Secure Systems”, 8th ACM Symposium on Operating System Principles; pp. 12-21; Asiloma, CA; December 1981; (ACM Operating Systems Review, Vol. 15, No. 5).

Schaefer, M. (2004) “If A1 is the answer, what was the question? an edgy naif’s retrospective on promulgating the trusted computer systems evaluation criteria”, In Annual Computer Security Applications Conference, pages 204–228. IEEE Press, 2004.

Schotanus, H.A., et al. (2011) “Decomposition of the Security Requirements for Connected Information Domains”, Military Communications and Information Systems Conference, Amsterdam
Vanfleet, W.M., et al. (2005) “MILS: Architecture for High-Assurance Embedded Computing,” STCS CrossTalk

Smulders, A.C.M. (2010) “Classification as a bottleneck for information sharing”, VOVKLICT January 2010.

Verkoelen, C.A.A., et al. (2010), “Security shift in future network architectures,” Information assurance and cyber defence, NATO IST 091, 2010.