Concept for trusted binding of metadata to data

Tor Gjertsen

Norwegian Defence Research Establishment (FFI)

27 February 2013

FFI-rapport 2013/00547

1176

P: ISBN 978-82-464-2226-8
E: ISBN 978-82-464-2227-5

Keywords

Informasjonssikkerhet

Informasjonsmerking

Approved by

Rolf Rasmussen	Project Manager
Anders Eggen	Director

Summary

Information exchange is a critical part of military operations. Information flows between domains are traditionally managed by air gaps and manual review-and-release procedures. More efficient information flow mechanisms are needed.

This report discusses the issues around secure marking of information, where the tag (metadata) can be bound to the data with a digital signature. It is proposed a concept as to how this can be done. The concept can be realized with available technology and to an acceptable cost, but development of new operational concepts will be required. The report is not about the implementation, but the MILS architecture seems as a promising starting point for the realization of the concept.

Sammendrag

Informasjonsutveksling er en viktig del av militære operasjoner. Informasjonsflyt mellom ulike domener har tradisjonelt måttet løses ved luftgap og manuelle inspeksjonsprosedyrer. Det er stort behov for mekanismer som muliggjør mer effektiv informasjonsflyt i slike tilfeller.

Denne rapporten diskuterer problemstillinger rundt sikker merking av informasjon, hvor merket (metadataene) bindes til informasjonen med en digital signatur. Det foreslås et konsept for hvordan dette kan gjøres. Konseptet kan realiseres med tilgjengelig teknologi og en akseptabel kostnadsramme, men det forutsetter at det utvikles nye operative konsepter. Det tas ikke stilling til valg av implementasjon, men MILS-arkitekturen ansees som et lovende utgangspunkt for en realisering av konseptet.

Contents

Preface

I will thank my colleagues, Nils Agne Nordbotten and Raymond Haakseth for good discussions in the process of writing this report. This is my very last report at FFI, as I am now retired. Further discussions with me on this topic will therefore not be possible, but I assume that my colleagues will be pleased to take part in such discussions.

1 Introduction

Information exchange is a critical part of military operations, and there is an increasing demand for information flows between domains. If domains are separated by a security span (e.g. Secret to Restricted), NATO security policy enforce rather strong assurance requirements on critical components involved. Traditionally air gaps and manual review-and-release procedures have been used. More efficient information flow mechanisms are needed to support future operations.

Secure marking of electronic documents is essential if the documents later are to undergo some sort of automatic testing, for instance in a security guard. The marking as such is assumed to be a process of binding a security label cryptographically to the document by using a digital signature. The label or the digital signature will not be discussed in this document. They will be chosen for the organization or domain in question.

It will be an advantage if NATO standardize on a security label for information exchange within the organization. In that case also a common infrastructure for providing services for handling of digital certificates has to be established. A public key infrastructure (PKI) is a system for the creation, storage and distribution of digital certificates, and establishing the trust so it can be verified that a particular public key belongs to a certain entity. With a NATO PKI and a common understanding of the labels it will be possible to send marked/signed information between NATO nations, for instance in a coalition operation via a security guard. This will also require a common understanding of user identities and user privileges in the overall scenario, to answer the fundamental question: can the originator be trusted?

In some scenarios it can also be useful to have an arrangement with a “local PKI” and a label, signature and security guard with only local significance. This will be much simpler to implement and administrate, but still you have the advantage of controlling what goes out of the domain.

The format of the security label can be generic, but the content of the label depend on the information and the operational scenario. An initiative has been taken in a NATO research group in specifying an XML-label and binding mechanisms for this that is assumed can be used; see (7) and (8).

This work is about enabling secure flows of information between security domains. It does not consider the information transport. The objective of this work is to discuss the provision of sufficient trust in the input to a security guard. Guard concepts and implementations are out of scope for this work. However a MILS-based solution is discussed in 4.3 based on experiences from earlier security related work at FFI on the MILS architecture.

2 Background

Information systems used to handle and exchange information is typically standard systems. Even in a military scenario that is often the case although you will also find “command and control

systems" specially made for military use. The cases for all these systems are that they traditionally have operated in "System High" mode and not in "Multi Level Secure" (MLS) mode and as such have no assurance requirements for confidentiality. The consequence of this is that if you mark the information within the application, you do not have sufficient assurance to really know what information is marked and signed. Even a System High-system may contain information of different classifications, and when low classified information is marked, because of insufficient trust, there is a risk that some high classified information can being included unintentionally.

3 Technologies

There are different technologies available to gain trust of a system. Formal trust and assurance is one thing, but also good development practice will enhance the quality of a system even if it does not undergo a formal evaluation.

3.1 Multi-Level Secure systems (MLS)

In an MLS-system, the system has sufficient trust to mark all information within the system, and the system is approved for this. The information can be processed and the resulting information can be remarked in a trusted way. So ideally the marking of information should be made in an MLS-system. Then you have full freedom to process the information, and all information will be correctly marked. However the availability of certified MLS-information systems is very limited. There are some MLS operating systems, but they typically reflect "old technology" and they are rarely updated because of the cost to do so. Complete MLS-information systems are typically built on the top of an MLS operating system, but they have to be evaluated and certified as complete systems, and the cost to do so is very high. Therefore it is likely that most military information systems also in the future will be operated System High. Systems set up to handle very high classifications will normally operate in "Dedicated" mode, and not connect to other systems. Multi domain and partitioned mode are being discussed, but do not change the basics and the fundamental problems of handling classified information.

3.2 MILS

The MILS architecture (Multiple Independent Levels of Security) is seen as promising for military systems with assurance requirements. Several vendors provide MILS-based technology with high assurance as a goal (Common Criteria EAL 6-7). One product have been certified (from Green Hills) for Power PC platforms. However the other programs in evaluations have been terminated due to a change in NSA's policy regarding evaluating operating systems and high assurance components in general. The current US policy when it comes to high assurance evaluations is that they will evaluate complete systems. Components will only be evaluated for low assurance levels, see (4) and (5).

The main component in the MILS architecture is the trusted separation kernel. This separates the system on a physical computer platform into partitions. In addition to strong separation, the MILS

separation kernel also provides for controlled information flow between partitions. It supports separation of both trusted and untrusted partitions. MILS vendors typically also provide virtualization software for some common operating systems like Linux and Windows in addition to the company's own proprietary real time operating system (RTOS). The MILS architecture makes it possible to divide a system into smaller modules, so trusted modules can be made as small as possible. The implementation and evaluation of trusted partitions have to be done separately. MILS only provides security functions for separation and flow control, and trusted partitions must be implemented and evaluated independently.

The MILS technology stems from embedded systems with high safety requirements, in particular used by the avionics industries. They have their own standardized evaluation criteria for safety and most of the separation kernels have been certified according to the standard DO-178B (9), with class A as the highest level of safety. This standard is about the software developing process. Another standard, ARINC 653 (6), is related to integrating many applications on the same physical processor in a safe way. This standard introduces virtualization and partitioning of applications. The ARINC architecture is similar to the MILS architecture. A major difference is that the MILS kernel has less functionality, i.e. much smaller size, enabling certification of the MILS kernel to a higher assurance level.

3.3 TPM

TPM (Trusted Platform Module) is both the name of the specification and the implementation of it, the TPM chip or the TPM device. TPM is often associated with Digital Rights Management. However it is also a more generic security concept. TPM provides basic security mechanisms like protected storage areas, computation of cryptographic functions and attestation of integrity measurement. Interesting in this context is that TPM can be used to ensure the integrity of program modules.

To our knowledge TPM has not been evaluated for high assurance levels that may be required to protect classified information. However there is at least one chip that has been evaluated to EAL 4 (moderate assurance).

For "single-level systems" there will not be hard assurance requirements for the software. Maybe in such systems TPM will be "good enough" to protect the critical software from being changed, for instance software for security marking of information.

4 Concept

This section is an attempt to sketch a concept for secure marking that is realistic to implement with available technology and to a reasonable cost.

4.1 Some conceptual considerations

It is assumed that future military information systems will still operate System High, and handle information of different classifications. Automatic marking in such a system will be dictated by the policy that all information will be set to the highest classification handled in the system, for instance to "secret" in a System High Secret system.

All marking lower than that will imply manual operator intervention. This manual process has to be trusted to some assurance level, depending on the security span in question. Information can be exchanged between System High systems belonging to the same domain and security policy without marking and Guard filtering.

In Single level processes/modules information can be marked automatically to the level of the module. However the marking has to be controlled in a module with sufficient assurance, to verify that the marking and confidentiality level is correct for the single level module.

Designers of future systems have to make the best out of what is available. Security critical modules may have to undergo a formal security evaluation, according to Common Criteria (NATO requirements today).

What can be "played with" in the design process of a system?

- Splitting up the overall system into smaller modules
- Single level modules have some advantages when it comes to automatic marking of information
- Security critical modules should be made as small as possible, since they have to undergo a security evaluation
- Information flows between systems and between modules within a system must be controlled (strongly). How this is done is a matter of implementation. Use of diodes can be part of a solution, as well as the use of MILS separation kernels. Integrity and/or encryption mechanisms can be necessary to protect the information in the flows.

"The solution" for secure marking should contain both legacy systems and future solutions. The goal is to be able to mark as much as possible automatically. However, it is assumed that for a long time, manual marking will be part of the overall solution. All information that is to be exchanged with other systems/domains has to be marked. A security guard will filter such information exchange.

Marked and signed information (digital signature) is "self-protected" and can be stored in an untrusted System High system as a marked item. As long as the information is unchanged and the signature is not broken, such items can be re-exported as marked items.

When it comes to military systems, it is not expected that the security policy will change radically when it comes to requirements for assurance. The challenge for planners will be to use what is

possible in a creative way. It is not expected a breakthrough for MLS-systems. The availability of such systems will be limited also in the future.

4.2 Chosen concept

"Secure Marking" is not an easy task. The availability of high assurance technology is expected to be low, and it is very expensive to evaluate a complete system from scratch. The idea of compositional evaluation has not reached a maturity level necessary for practical use, so evaluations still have to be done system wise.

Then, given the current situation, what is the best that can be achieved with available technology? The following sections introduce elements and sketches to a solution.

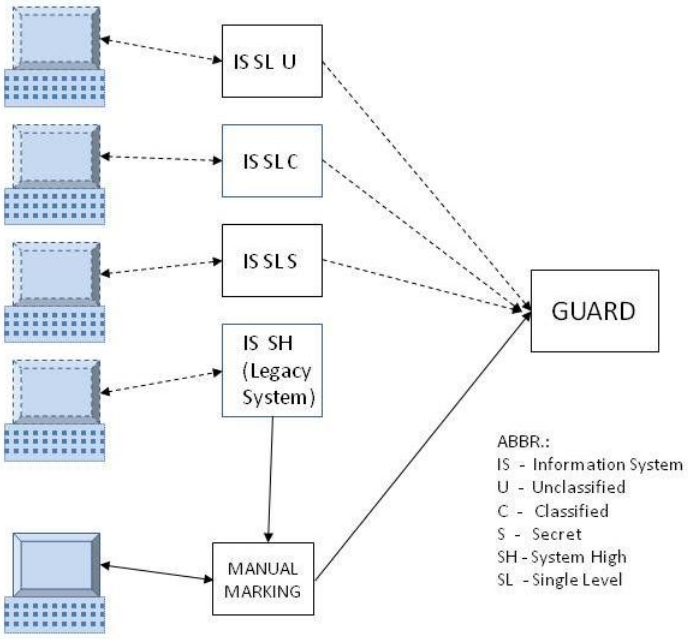

Figure 4.1 Principle sketch of secure marking

Figure 4.1 contains some single level (SL) modules. As said before, such modules can provide secure automatic marking (of correct confidentiality level). Further it shows a legacy system module operating System High (SH). This takes care of the migration from existing systems in operation to future systems in operation.

A manual marking process has been introduced, to serve the legacy system. This will require a dedicated terminal function. The information flows between the terminal and the marking function have to undergo a strict control including integrity, so "what you see is what you mark".

If the single level modules require terminal functions, they will also require dedicated terminals, unless a trusted terminal switch is provided.

For the completion of the view, also a guard is shown, since this is the main reason for marking the information. In a real scenario it can be multiple instances of both guards and networks. It will also be an information flow the opposite way through the guard in a general case. For simplicity this is not shown.

The single level systems can send information directly to the System High system as long as the classification of the information does not exceed the highest classification of the System High system and they belong to the same domain. This information can be marked or unmarked. Information flows between systems are not shown in the figure.

Military command and control systems are typically running in System High mode of operation, for instance in System High Secret. In the concept such legacy systems can be run unchanged. The security policy will in such systems dictate that all information by default have to be handled as secret and all automatic marking has to be set at that classification level. Other levels will require a manual marking. Such "manual marking" has to be done by a trusted unit, outside the legacy system.

The format of this marking has to follow agreed standards and methods, such that the marking can be verified and tested and filtered by a security guard when exporting information to another domain.

Marked information is sealed cryptographically by a digital signature and bound to the information, so the information is "self-protected". As long as the seal is not broken, the integrity of the information and the label is conserved and can be tested. Therefore marked information can be stored securely in an untrusted System High system. The security is contained in the information itself, and do not rely on the system that store the information.

Marked information can be exported from all kinds of systems (single level, multi level, system high etc.), via an approved security guard that enforces the security policy and tests the security mark and the integrity of the information.

If an information system processes marked information to produce new combined information, the new information has to be marked as a new object. In a single level system that can be done automatically. Information from a System High system has to be marked in a trusted manual marking function.

4.3 The marking process

The implementation of manual marking has to provide "what you see is what you mark". This will put requirements to the solution of the dialog between the screen/terminal and the marking process. It is assumed that this solution has to be trusted and the integrity must be preserved in this dialog.

The documents to be marked can be of different types and formats, for instance e-mail, military messages or attachments. For complex documents like MS Word or Power Point special attention has to be taken. Handling such documents will require rules and strict control of how these are configured. This is a general problem that also applies to existing systems and solutions, but this has probably not gotten sufficient attention in the past.

Such types of documents may contain a lot of hidden information created in the process of writing the document. It is not obvious which information is marked. The document may contain information that is not visible in the first place and not at all intended for the other party in an information exchange. Special attention should be taken when configuring such applications in scenarios where the information is going to be exchanged with other parties. In complex documents, what you see is not necessarily what you sign.

The goal for future military operations in NATO is the so called Network Enabled Capability (NEC). This implies a flexible information network, where the access to timely information on all levels in the organization is vital. In this scenario all manual interaction will be contradictory to the overall operation. However, use of legacy systems in combination with new solutions obviously will require some manual interaction in the marking process.

4.4 A MILS-based implementation

This report shall in principle not deal with the implementation of secure marking. However the MILS platform has some interesting characteristics which are discussed in the following.

Figure 4.2 shows a MILS-based implementation of the concept. The different modules are hosted in separate partitions, and the MILS separation kernel will provide controlled flows between the modules.

The motivation for selecting a MILS-based solution can vary. If there is a need for a terminal-function to any of the single level partition or the legacy system, then a secure MILS terminal function would be an advantage, since this can access modules of different classifications, and one single terminal can do the job towards all the modules. The secure terminal can be implemented as described in (1) and (2). (3) gives some more general background for this technology.

Further the MILS separation kernel will provide controlled information flows between the partitions so the need for dedicated lines and diodes is eliminated.

The manual marking module has to be trusted, to some level of assurance. In a MILS solution, the trusted modules can be made very small. If they are implemented on the top of the “native “ minimum runtime interface of the separation kernel without any big virtualized operating system, this will ease the security evaluation.

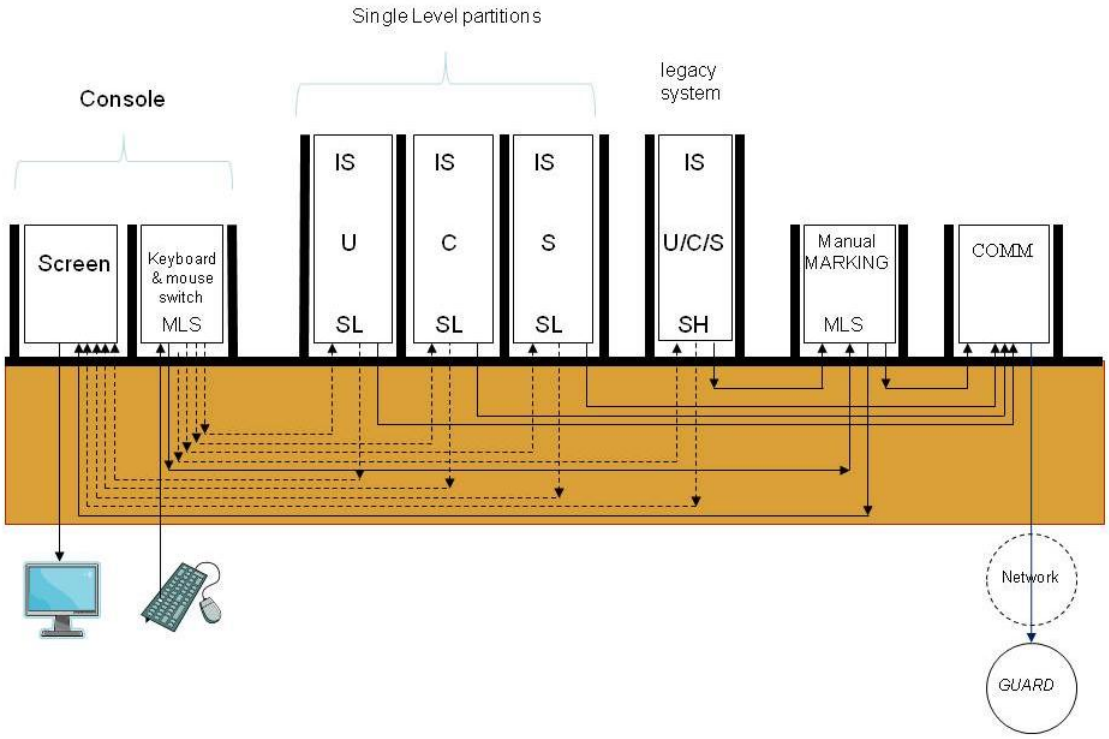

Figure 4.2 A MILS based solution to secure marking, principle sketch

5 Conclusions

The ideal and conceptual simple solution for secure marking of information would be to upgrade legacy systems to operate multilevel. However it is assumed that this will never happen because of the cost to do so. The upgrade and following security evaluation would not at all be a simple task.

Existing military information systems have to a great deal emerged as an automation of existing operational procedures. This has led to complex command and control systems operating in System High mode. This complicates information exchange.

In the future to construct an information system that to a great extent consists of interconnected single level systems, will be a great challenge. The overall design and operational concept for the system must be given much attention. It has to be redesigned completely compared to existing systems and operational thinking. The challenge will be to have a flexible utilization of single level units in a multilevel setting, and to minimize the need for manual interaction.

Independent of the chosen concept, it is expected that some critical modules will have to undergo a security evaluation. To evaluate complete systems to the assurance level that will be required for "multi level" systems is assumed to be very expensive, and consequently not realistic. This work is not about implementation, but one technology is mentioned, MILS. MILS do not solve the fundamental problem of classified information handling and exchange. But it may help to divide a complex system into fragments that can be manageable for a security evaluation.

References

(1) Nils Agne Nordbotten and Tor Gjertsen, Towards a certifiable MILS based workstation, FFI-rapport 2012/00049

(2) Tor Gjertsen and Nils Agne Nordbotten Military Operational Systems in Field – Multiple Levels of Security FFI-rapport 2009/01137

(3) Tor Gjertsen and Nils Nordbotten, Multiple Independent Levels of Security (MILS) - a high assurance architecture for handling information of different classification levels, FFI-rapport 2008/01999,

(4) NIAP, "SKPP Sunset Q&A," [Online]. Available: http://www.niap-ccevs.org/announcements/SKPP Sunset Q&A.pdf. (Accessed February 2013).

(5) NIAP, http://www.niap-ccevs.org/cc-scheme/pp/pp.cfm/id/pp_skpp_hr_v1.03 (Accessed February 2013).

(6) Slawomir Samolej, ARINC Specification 653 Based Real-Time Software Engineering

(7) Anders Eggen, Raymond Haakseth, Sander Oudkerk and Andreas Thummel, XML Confidentialty Label Syntax - a proposal for a NATO specification, FFI-rapport 2010/00961 (NATO UNCLASSIFIED)

(8) Anders Eggen, Raymond Haakseth, Sander Oudkerk, and Anderas Thummel, Binding of Metadata to Data Objects - a proposal for a NATO specification, FFI-rapport 2010/00962 (NATO UNCLASSIFIED)

(9) RTCA (www.rtca.org, formerly Radio Technical Commission for Aeronautics), DO-178B, Software Considerations in Airborne Systems and Equipment, issued 12-1-1992