Medical Informatics Europe '99
P. Kokol et al. (Eds.)
IOS Press, 1999

Experiences with a new Security Standard for Healthcare Information Systems

Kees Louwerse, Margot van Ditmarsch, Erik Flikkenschild
Leiden University Medical Centre (LUMC)
Central Information Processing Department (CDIV)
P.O. Box 9600, NL 2300 RC Leiden

Abstract. This article describes the results of the implementation and demonstration of the Standard CEN ENV 12924 (Security Categorisation and Protection of Health Care Information Systems), that was performed as part of the ISIS/MEDSEC project of the EU. The categorisation scheme given in the standard was followed through for almost all information systems or sub-systems in the Leiden University Medical Centre. The status of the security measures was evaluated for ten systems; further implementation plans were then drawn up for these systems, and partly effectuated. Findings are reported, both on the present security level, and on the applicability of the standard (which in general was found to be very positive). In the course of this work, use was made of a database support tool, developed in an earlier EU project (SEISMED).

1. Introduction

Information systems nowadays play a very important role in patient care, and malfunctioning of these systems may become outright dangerous to the patient. Nevertheless, in many cases not enough attention is paid to the security of these systems. In recent years, several tools have become available which should help improve this situation.

One of the results of the working programme of CEN/TC251 (Medical Informatics) was the standard for Security Categorisation and Protection for Healthcare Information Systems, which was formally adopted in 1997 by CEN as a pre-standard (CEN ENV 12924 [1]). As part of the MEDSEC project [2] (which forms part of the ISIS programme of the European Union), a first demonstration and implementation effort was performed in Leiden.

This standard contains a security categorisation model for information systems in health care, distinguishing six categories, plus some refinements. For each category it specifies the required protection measures. The project task consisted of demonstrating and implementing (as far as possible within a limited period) the standard in a real life situation, and providing feedback on these results to the CEN organisation. An overview is presented here.

2. CEN ENV 12924

The standard provides a method for categorising Health Care Information Systems according to their security requirements. Taking into account the different aspects of Integrity, Availability and Confidentiality, six categories are distinguished. For each category a comprehensive set of protection measures is specified.

Apart from these 6 categories, the standard also allows for different environmental and connectivity factors (6 classes for physical environment, 3 classes for physical connectivity, and again 3 classes for the logical connectivity).

3. Categorisation

To perform the categorisation, a series of interviews was held with the managers of all concerned sub-systems (this involved at least the technical manager, but quite often also his counterpart on the user side). About 30 persons have been interviewed, giving information about 91 sub-systems of the central Hospital Information System and 21 other systems.

A summary of the results is given in the table below.

Table 1 - Security categories

category	availability	confidentiality	integrity	number of systems	
				HIS	other
I	non-critical	sensitive	non-critical	1	8
II	non-critical	sensitive	critical	7	4
III	critical	sensitive	critical	2	3
IV	non-critical	very sensitive	non-critical	12	1
V	non-critical	very sensitive	critical	19	1
VI	critical	very sensitive	critical	22	0
none	..	non-sensitive	..	26	4

The systems, for which the category is indicated as 'none', are the ones in which no confidential data are handled. For non-HIS systems the sample is not complete.

This categorisation exercise led to the conclusion that the categories are relevant, and sufficiently varied for the purpose; the categorisation scheme can well be used in practice.

Some suggestions for improvement were made, like adding an extra category (confidentiality non-sensitive, critical for the other aspects) with a corresponding protection profile, and improving the definitions of some of the terms used in the standard.

Our experience indicates, that the necessary information for the categorisation step can be easily obtained in the course of a brief interview with the responsible person(s).

4. Selection of sub-systems for further investigation

From the complete set of systems, a selection of 10 was made, for which the (present and future) applicability of the standard was investigated in detail. In making this selection, we tried to obtain a representative cross-section of the types of system in use in the Centre.

5. Detailed examination of the selected (sub)-systems

Using the standard, an inventory of the present situation with respect to information security was made for all the selected systems. A further series of interviews were held with the responsible system managers. During these interviews, the recommendations given in the standard were discussed, and the current status for the actual system was recorded. For the status, one of the following indications was used: high priority / include in this year's plan / include in next year's plan / still under discussion / partially implemented / already (fully) implemented / accept the level of risk / not applicable (for specified reasons).

6. Bookkeeping with the SIDERO model

For each system, a detailed report on the results has been written, including:

- an implementation plan to make the system compliant with the standard, as far as is considered necessary, and
- an analysis of the suitability of the standard for this type of system.

The implementation plans have been initiated or even (partly) effected, as far as time and required effort allowed.

In order to facilitate bookkeeping of the findings and results, these were recorded in the measuring instrument SIDERO [3]. This is essentially a database model for security guidelines and measures, which was developed during an earlier EU project (SEISMED [4]).

This tool was adapted for the present purpose by adding the recommendations from the standard as a table to this database. For each system, a quantitative description was produced of the current protection status, as compared to the standard. The database provided an easy means of producing reviews, e.g. for each status separately. These reports were discussed in detail with the responsible system managers, and on the basis of this discussion, action plans were produced, indicating the time scale on which appropriate measures would be effected, or in some cases, explaining e.g. that a certain measure would not be applicable in our case.

7. Examination on how well the standard is adhered to at present

On the basis of the examinations, we could form a good picture of the present security situation for the various sub-systems. Details were collected in separate (confidential) internal reports for each system.

Briefly summarised, the results can be given as follows:

- the standard does provide an sufficiently complete set of measures for the systems considered; only a few relevant measures were found which could not be fitted within the context of the standard;
- for the systems considered, a significant part of the requirements from the standard had been fulfilled, some would be implemented in the near future; but of course, some work remains to be done;
- in several cases, a requirement could not be realised within the technical scope of the present system; weak points in the protection usually were concerned with:
  - access control (usually only a password mechanism is available; procedures for managing and using passwords are improving, but are still relatively poor);
  - logging facilities (usually mainly aimed at recovery, and not providing sufficient facilities for tracing what has happened);
  - protection procedures, (non) use of encryption; and
  - back-up provisions;
- there were many examples, where facilities offered by suppliers in their products are not sufficient at present to enable the users to conform to the standard;
- in a few cases, the requirements from the standard are considered as being too strict.

In general, it was found that the protection level of the centralised systems was reasonably close to the prescribed situation, although there were some clear exceptions, as mentioned above.

For the various departmental systems, we have encountered different situations, but in

general the protection level was significantly lower than for the centralised systems.

On the whole, however, all persons interviewed agreed that the level indicated by the standard was appropriate, and should be taken as the target.

8. Conclusions

Our overall conclusion is that the standard CEN ENV 12924 provides a very useful instrument for evaluating and improving the security situation in Health Care Information Systems. Although it should not be considered as a substitute for a formal Risk Analysis, it may well serve as a tool for a first evaluation of the information security status of health care environments, and indicate where improvements are most urgently needed and effective. It can also highlight the places, where a more thorough Risk Analysis would be mandatory.

Some suggestions have been made for amendments in a few of the recommendations in the ENV; e.g.: inclusion of a seventh information category (confidentiality non-sensitive, but critical for the other aspects) would provide a more complete picture.

The effort within the MEDSEC project has been limited to experiences within one hospital in the Netherlands (with some additional work at a major German hospital). It would be worthwhile setting up a broader evaluation of the standard to verify the present findings, also taking into account some other categories of health care institutions. In our opinion, after such a further verification, this document should be recommended to serve as a basis guideline for information systems security in European health care.

The practical use of the standard is simplified significantly by the use of a bookkeeping tool (like we have used SIDERO).

Available information systems from vendors usually do not offer sufficient functionality to implement all requirements from the standard. Wide acceptation of the standard, preferably made mandatory by national regulations, would increase the possibility of getting such features realised in future versions.

References

[1] CEN ENV 12924 (Security Categorisation and Protection of Health Care Information Systems); CEN, Brussels, 1997

[2] MEDSEC (Health Care Security and Privacy in the Information Society): European Commission ISIS Programme; deliverable 27: Demonstration Results for the standard CEN ENV 12924
More details about the ISIS programme can be found at http://www.ispo.cec.be/isis/

[3] SIDERO: E.L.A. Flikkenschild and C.P. Louwerse, The Implementation of Security in the Health Care information Systems, closing the gap between theory and practice. In: R.A. Greenes et al. (ed.): Proceedings MEDINFO '95 (Vancouver), ISBN: 0-9697414-1-3. North Holland, Amsterdam, 1995, pp. 648-651.

[4] SEISMED consortium: Data Security for Health Care (handbook; 3 vols.), ISBN 90 5199 263 7. IOS Press, Amsterdam, 1996.
The SEISMED project (Secure Environment for Information Systems in MEDicine) was initiated in 1992 within the context of the AIM-programme (Advanced Informatics in Medicine) of the European Commission. One of it's important products was this set of three handbooks, providing guidelines for several aspects of information security in Health Care Information Systems.