TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 15300

October 2006

English Version

Health informatics - Framework for formal modelling of healthcare security policies

Informatique de santé - Cadre pour modélisation formelle des politiques de sécurité dans le domaine de la santé

Medizinische Informatik - Rahmenkonzept für Modelle von Sicherheitspolicen im Gesundheitswesen

This Technical Report was approved by CEN on 5 December 2005. It has been drawn up by the Technical Committee CEN/TC 251.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36   B-1050 Brussels

Ref. No. CEN/TR 15300:2006: E

Contents

Foreword

This document (CEN/TR 15300:2006) has been prepared by Technical Committee CEN/TC 251 "Health informatics", the secretariat of which is held by NEN.

This non-normative CEN Technical report is intended to help the European health sector understand the need for serious work on formal models dedicated to provide healthcare-relevant security policies. This very first step towards European recommendations and/or standards about healthcare security policy formal modelling is only a small part of the twin theoretical-pragmatic approaches that are to be developed in order to help the healthcare sector end user implement his own relevant security policies.

Introduction

In order to help the healthcare sector specificity to be taken into account in any security policy specification and implementation it is necessary to consider the three following aspects:

• it is *unavoidable* to be as close as possible to the *user requirements* (i.e. informal but also technical requests);

• it is *necessary*, in consequence, to be adaptable enough in order to be able to catch all those various possible requirements, in the sense that it is mandatory that the approach to security policy specification need to have high flexibility property;

• it is *obliged*, at the opposite, to be rigorous enough when deriving such requirements into some refined security policies, in the sense that it is also obliged that the methodology need to have high robustness capacity.

User requirements

Most of the time the user requirements, concerning the security aspects, if not helped by any comprehensive standard and/or some detailed security expertise, are not formal and/or detailed enough to be directly or even automatically derived into security policies; especially in such a specific sector as the healthcare activity.

In any case, these are the security requests and requirements which are to be progressively refined in order to be implemented. In addition, due to the wide range of actors, profiles, roles but also of IT technologies, communicating systems, and security technologies, the user requirements might belong to a wide spectrum of possible requests: this is the flexibility necessity. Nevertheless, any case of such user requirements, concerning the security aspects, need to be proved as correctly taken into account: this is the robustness obligation.

Flexibility

Considering:

• the four possible security properties possibly required (availability, integrity, confidentiality and auditability);

• times, the different IT systems possibly considered,

• times, the various healthcare establishment types and categories,

• times, the varying healthcare organisations and procedural processes,

• times, the variable healthcare actors and their related roles,

• times, the potential security technologies useable and used,

• times, the possible distribution and sharing policies of healthcare information,

it is clear that a very high number of authorised security policies might defined, refined and formalized.

In order to capture all these case, better than an exhaustive enumeration, an implicit definition by means of some modelling approach should be easier and more faithful: the high diversity of security policies can only be captured by a high flexibility of the security policy expression and formalising facilities: that is an overall necessity.

Robustness

Considering:

• the always possible accidental and/or intentional (malicious or non-malicious) failures in the security policy definition /specification/conception/implementation process;

• the always possible accidental and/or intentional (malicious or non-malicious) misuse of any healthcare information system;

• the always possible accidental and/or intentional (malicious or non-malicious) misunderstanding of the security needs of any healthcare organisation expressing informal security requirements;

• the always possible accidental and/or intentional *a posteriori* conflict between two healthcare parties involved in a same health activity or health information exchange;

• the always possible security failures integrating in any security component being part of a global solution

it is clear that a high level of trustworthiness is required when the security policies are defined, refined and formalized.

In order to capture such high a level of trustworthiness, better than repetitive controls, an proved strategy/process should be more trusted and more relevant: the high level required for the security policy expression and formalising can only be captured by a high robustness of the security policy expression throughout mathematical facilities: that is an major obligation.

1   Scope

This CEN Technical report specifies the starting point for working on some formalising tools that could be used by the healthcare actors to express, compare and validate local and/or network security policies.

Defining and validating a correct security policy encompass different activities such as expressing correctly (i.e. without any ambiguity), formulating correctly (i.e. without any misinterpretation) and proving the correctness (i.e. without known failures or major lack) of the [to be formally modelled] security policy.

This CEN Technical report does NOT intend at all to specify a UNIQUE or UNIVERSAL formal model that need to be used by the European healthcare community: it only indicates, as a first working step, some ways that could be followed to help that healthcare community to correctly and fruitfully manipulate the security policy concept(s) and the formal modelling techniques.

This CEN Technical report does NOT intend to indicate an EXHAUSTIVE spectrum of all the published formal security policy models: it only gives a readable and understandable flavour of the most well-known formal models and also of the [maybe] most interesting ones from the healthcare activity and needs point of view. This CEN Technical report is, in this very first version, divided in five parts:

• *Part #1 - Introduction to formal modelling*: this clause summarises and justifies the following needs:

i. need for **policies**, in general and for any context;

ii. need for **security** policies, in any data processing context;

iii. need for **models** (or *modelling facilities*) *of security policies,* in some generic system environments;

iv. need for **formal** models (or *formal modelling facilities*) *of security policies*, in some sensitive areas;

v. need for **healthcare**-*oriented formal models of security policies*, specialized to healthcare specificities.

• *Part #2 - Historical security policies and models*: this clause explains and introduces the main objectives and concepts of the security policy modelling activity that seems to be of interest for future healthcare usage:

a. formal models of confidentiality policies;

b. formal models of integrity policies;

c. formal modelling attempts of general purpose policies.

• *Part #3 - A generic formal modelling approach*: this clause informs on the possibilities of formal models, related to the security policy activity and especially for the healthcare organisations:

a. which types of formal models exist?

b. why using formal modelling?

c. what for choosing modal logic?

c. how implementing deontic logic?

• *Part #4 - Healthcare current needs and future trends*: this clause intends to make the link between all the user requirements that are handled inside the activity of CEN/TC 251 and the past/current/future needs:

1. past results with the security categorisation work;

2. *current* work with the distribution- or the communication- security policy modelling;

3. *future* trends and corresponding expected results with the new activity on real formal modelling.

• *Part #5 - Healthcare applications of FM_HSP*: this clause gives examples of applicability of the global formal modelling approach to healthcare security policies:

1. *anonymisation* policies;

2. *Trusted Third Party's* policies;

3. *communication security* policies;

4. *cryptographic* policies;

5. *safety versus security* policies.

This CEN Technical report is intended to built a long term prospect: this means that confidentiality and integrity, but also availability and accountability, considerations need to be taken into account in order to propose interesting and useful results to the healthcare actors concerned with the general security policy aspects.

2   Normative References

Not applicable.

3   Terms and definitions

For the purposes of this CEN Technical report, the following terms and definitions apply.

NOTE   Please note that for those definitions where no reference is given, the definitions proposed here have not been endorsed to be generally valid in the work of CEN/TC 251.

3.1
access control
a means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways
[ISO 2382-8:1998]

3.2
accountability
the property that ensures that the actions of an entity may be traced uniquely to the entity
[ISO 7498-2:1989]

3.3
anonymity
property that ensures that the nominative identity is not revealed

3.4
auditability
the property that ensures that any action of any security subject on any security object may be examined in order to establish the real operational responsibilities
[ENV 13608-1:2000]