Using Process Models to Analyze Health Care Security Requirements

Susanne Röhrig
secunet SwissIT AG
Solothurn, Switzerland
roehrig@swiss-it.ch

Abstract— **Even though most information systems need to be secured in a cost-effective manner, "appropriate" security is difficult to specify. This article presents an approach to re-use existing business process descriptions for the analysis of security requirements and later the derivation of necessary security measures. The applicability of this approach will be proved with an example from the health care sector.**

I. Introduction

As the use of information systems for sensitive purposes increases, the demand for appropriate security measures rises. Unfortunately, security and appropriate security measures are difficult to specify. Though some security standards aim at providing appropriate security controls, most do neither specify what "appropriate" means nor provide any guidance for an organization to decide upon the term. Gaskell [1] even states that *"it is not possible to define upfront what "appropriate" is in every situation"*. The aim of the method presented in this article is to provide an aid to decide which security safeguards are appropriate when certain security objectives shall be reached. Business process models are used to analyze these security requirements. The resulting catalogue of safeguards can be used when newly implementing a process on a computer system or for auditing purposes.

During the analysis of business processes the following is recorded: the place where data are kept and stored, where they are sent, who processes them and who accesses them. This makes the flow of information and who is able to access or change data more transparent. Therefore, it can be used to determine which safeguards must be taken where and by whom to provide for an appropriate level of security.

The remainder of this article is structured as follows: After a review of related work (section I-A) and the research context in which is work is embedded (section I-B), terms related to security and business processes that are used in this article are defined in section II. Section III describes the ideas of the proposed POSeM method (**P**rocess **O**riented **Se**curity **M**odels) focussing on two rulebases — one used to check for consistency and the other to derive "appropriate" security safeguards. After proving the method's applicability with a detailed example taken from the health care sector in IV, a discussion and an outline of further research steps are given in V.

A. Related Work

Current literature provides several different approaches concerning security of business processes and workflow systems. An overview of research concerning security of workflow systems, i.e. automatable processes, is given in [2].

An approach to integrate a threat and risk analysis within a method for business process and workflow modeling can be found in [3], [4]. Security is defined by the exclusion of quantifiable and qualifiable risks. Therefore, the procedure of modeling serves to implement security requirements that have been known beforehand.

A method based on business processes to examine security risks, identify and evalutate security measures is described by [5]. Simulation is used to analyze the effects of weaknesses on business processes and related security-relevant objects. So-called *"security subprocesses"* that need to be present for security reasons are depicted by [6]. In [7], [8] it is argued that security requirements vary with the perspective taken. The authors identify five different perspectives which are closely related to the elements of a workflow specification. In a further step, they define "ALMO$T", a language for modeling secure business transactions.

Chung [9] describes a process-oriented approach to represent security requirements as a special case of non-functional (or quality) requirements as potentially conflicting or harmonious goals and uses them during the develpment of software systems. Finally, in [10] the Use Case Models of the Unified Modeling Language are further developed into "Abuse Case Models" that are used to describe *"a complete interaction between a system and one or more actors, where the results of the interaction are harmful to the system"*. These models can be used to help in understanding the system's security requirements and designing security functions that prevent an abuse of the system.

Most approaches cited above focus on an analysis of risks or vulnerabilities. In contrast to them, the approach presented in this article models the procection objectives of the business process.

B. Research Context

The ideas presented in this article were initially influenced by the work of Holbein et al. [11], [12] who used workflow systems for the security design in organization and the subsequent implementation of access control measures. The workflow model was thus used to implement a

very strict mechanism to protect confidentiality. An implementation of this approach for a health care process was carried out during a research project funded by the Swiss national science foundation [13]. It focused on a process modeling a clinical trial of a new medication. The application developed during this project granted access to the involved persons on a strict need-to-know basis making the underlying process model a means to achieve confidentiality [14]. The use of process modeling to analyze all security requirements (i.e. not only confidentiality) of systems or processes in accordance with the company's security objectives was still widely unexplored.

The idea of analyzing different components of an e-business process for specific security requirements (i.e. for their requirements on confidentiality, integrity, availability, and accountability) is pursued in [15] and [16]. In [17] a method for deriving security safeguards from a requirements analysis is sketched for a process describing the conclusion of a contract using electronic media. Again four security objectives are pursued. This article takes these ideas a step further in explaining details of this method as well as illustrating it with a detailed example taken from the health care area. A complete description of the method presented here will be provided in the author's PhD thesis.

II. Definitions

A. Security

Generally, a **security objective** is the *"contribution to security that a system or a product is intended to achieve"* [18]. The term security objective must not be confused with **security service** that is defined in [19] as a *"processing or communication service that is provided by a system to give a specific kind of protection to system resources"*. Therefore, security objectives are the goals that are to be achieved while security services are means to achieve these goals. A security objective always refers to a certain quality or state of a computer system. **Confidentiality**, **integrity**, and **availability** have been identified as basic objectives of security in 1980 [20]. With the advent of electronic commerce more security objectives have been identified to suit certain legal needs; the most important one is **accountability**[1]. The four security objectives are defined as follows:

- **Confidentiality** describes the state in which data are protected from unauthorized disclosure. When talking of confidentiality of personal data the terms privacy and secrecy are often used; the former refering to legal aspects as defined in national data protection laws, the latter to *"the effect of the mechanisms used to limit the number of principals who can access information"* [22].
- Data **integrity** is defined as *"the property that data meet an a priori expectation of quality"* in [23], whereas system integrity is *"the quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system"*. Therefore, integrity means that neither data nor system have been altered or destroyed. We distinguish between accidental (e.g. transmission errors) and malicious (e.g. sabotage) modification.
- The term **availability** means that data and systems can be accessed by authorized persons within an appropriate period of time. Reasons for a loss of availability of a system may be attacks (e.g. abusing known system vulnerabilities) or instabilities of the systems and its components.
- **Accountability** of a system enables *"activities of a system to be traced to individuals who may then be held accountable"* [23]; thus when accountability is guaranteed, the participants of a communication acitivity can be sure that their communication partner is exactly the one he or she claims to be.

Security measures or **safeguards** are *"the protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards include but are not necessarily limited to hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices"* [18]. In this article the terms security measures and safeguards will be used synonymously.

A **security model** is according to [19] *"a schematic description of a set of entities and relationships by which a specified set of security services are provided by or in a system"*. The Acqua Book of the American National Computer Security Center (NCSC) [24] states that a security model *"precisely describes important aspects of security and their relationship to system behavior"*. It may contain the following parts:

- data structures and storage items
- processes[2] and subjects
- users and user roles
- I/O devices
- security attributes
- non-disclosure levels

B. Business Processes

The ideas of Business Process Reengineering (BPR) were conceived by [25] and [26]. By redefining the way tasks are carried out within an enterprise they aim to reduce cost and time, while at the same time improving quality of products and service. To this end, the process—as carried out—must be recorded using process models and be re-defined using process management mechanisms and tools.

In [27] a **process model** is defined as *"a description of a process expresed in a suitable* process modeling language*"*. The **process modeling language** in turn is defined as

[1] Several extensions to this scheme of four have been proposed; [21] even provides the four "new" security principles **responsibility**, **integrity**, **trust**, and **ethicality** to replace the classical security goals. For the purpose of this article, however, the "classical" scheme will be used to restrict the level of complexity of the model; of course, extensions are possible.

[2] The NCSC standards use the term **process** in a computer science sense *"a program in execution"* [23] in contrast to its business meaning where it denotes *"a specific ordering of work activities across time and place, with a beginning, and end, and clearly identified inputs and outputs"* [25].

"formal notation used to express process models, both for production processes and meta processes".

According to [28] the constructs that collectively form the basis of a process model are an **agent**, i.e. an actor or process participant (human or machine) who performs a process element, a role, i.e. a coherent set of process elements to be assigned to an agent as a unit of functional responsibility, and an **artefact**, i.e. a product created or modified by the enactment of a process element. A process consists of **process steps** (activities or actions) which are defined as atomic subprocesses with no externally visible substructure. In this article the term **process component** will be used to collectively describe actors, artefacts, and activities.

The description of a process is most commonly represented by the following four perspectives [28]:

- The **functional perspective** describes what process elements are being performed.
- The **behavioral perspective** represents when process elements are performed. This includes control structures like feedback-loops, iterations, decision-making conditions, entry and exit criteria etc.
- The **organizational perspective** describes by whom the process elements are performed and where they are performed. It also includes physical communication mechanisms used for transfer of entities, and the physical media and locations used for storing entities.
- The **informational perspective** that represents the informational entities that are produced or manipulated by a process.

A description language must therefore take into account all of these constructs and perspectives—at least. For the purpose of this article, security information (i.e. security objectives of process components) will be included, too. The term **workflow** is used to describe the automatable parts of a business process.

III. The POSeM Method

The method proposed in this article to analyze appropriate security measures from process models consists of four steps and an optional fifth one: First of all the general security objectives of the business process must be defined. A fine-grained view on these objectives will be the result of the next step where the security objectives of all constructs of the process, i.e. actors, process steps, and artefacts, are examined. A third step will examine whether these specifications are consistent and non-contradictory by means of a first rulebase (RB1). By using a second rulebase (RB2) that maps security measures to the specified security objectives a list of necessary security measures for each process component can be generated. Since these measures are on a very generic level, they can be joined with system information to generate system-specific measures in an optional fifth step.

Figure 1 shows an overview of this method and its steps. The next paragraphs will examine the four main steps of POSeM in detail. Chapter IV will illustrate them with a small example.

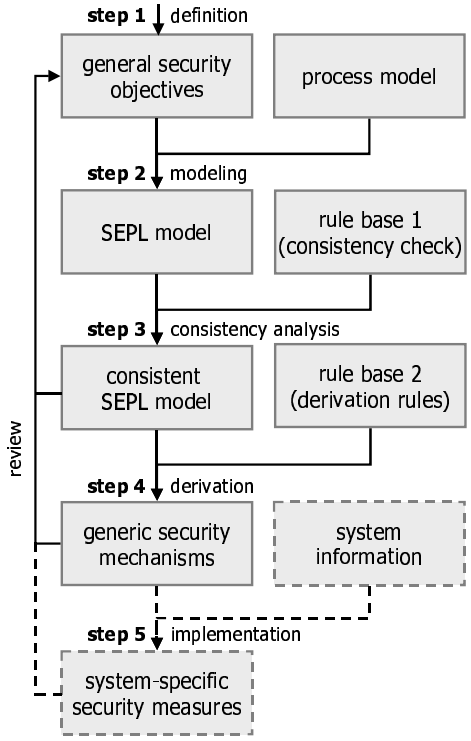

Fig. 1. Overview of the POSeM Method

A. Step 1: Definition of General Security Objectives

When starting a security analysis general objectives have to be specified. This means that not only the business aims but also the security objectives of the company must be explored. This can be a rather general statement that takes into account both the requirements of the industry the process is set in and the specific requirements of the business process under scrutiny. In this step it should also be examined whether the security objectives conflict with the objectives of the business in general or the objectives of this particular BPR activity, e.g. skipping data validation procedures in order to save time, which is likely to lower data integrity.

Result of step 1 will therefore be a general framework that aligns the security objectives to the objectives of the business process.

B. Step 2: SEPL model

Security objectives for all process components will be defined during step 2. In order to specify security requirements of business processes a language must contain constructs to define both process and security features. A simplified version of the Workflow Process Definition Language (WPDL) [29] was chosen to specify business processes and enhanced with security features and type markings to make up the Security Enhanced Process Language (SEPL).

In SEPL the following constructs exist: `PROCESS`, `ACTIVITY`, `TRANSITION`, `PARTICIPANT`, and `DATA`. While describing the process in SEPL this step also defines the security objectives for all components of the business pro-

cess, i.e. for the single activities (ACTIVITY), actors (called PARTICIPANT), and artefacts (DATA[3]). Process components generally have a unique identifier, a mnemoic name, and a textual description. Each activity and artefact is assigned its security requirements (i.e. the level of confidentiality, integrity, availability, and accountability that should be provided for it), and each actor is assigned a "clearance" level (i.e. the level of confidentiality, integrity, availability, and accountability) he or she is allowed to handle. These constructs are reflected in the description language, i.e. compared to WPDL the constructs DATA, ACTIVITY, and PARTICIPANT are extended with SECURITY_LEVELS or CLEARANCE_LEVELS. In SEPL five levels of security or clearance are defined (in descending order): VERY HIGH, HIGH, MEDIUM, LOW and NONE. Table I explains how the values of SECURITY_LEVELS and CLEARANCE_LEVELS for security objectives should be applied and gives some examples.

TABLE I
SEPL SECURITY LEVELS AND THEIR USE

SEPL level	application	example
NONE	the security objective has no impact on the process component	"confidentiality" of a web-site
LOW	if the security objective is hurt minor annoyances arise that can be overcome by other media	availability of e-mail
MEDIUM	if the security objective is hurt difficulties arise that might lead to financial losses	integrity of a commercial web-site
HIGH	violations of this security objective lead to legal problems, damage of (company) image as well as to high financial losses	confidentiality of customer data (subject to privacy laws)
VERY HIGH	violations of this security objective not only lead to high financial losses but might lead to loss of human life	integrity of patient data (dosage of medication)

If an artefact is assigned the integrity level HIGH, the final process implementation will provide safeguards that ensure a high security. In general, the level of any security objective for any process component is modeled as the security level that shall be achieved in the final process implementation. These semantics of the security levels are reflected by the rules in RB1 (cf. III-C).

The assignment of an actor to an activity as well as artefact to activity is defined within SEPL's ACTIVITY-statement, where references to the actor's and the artefacts' identifier(s) are made[4]. Table II shows an example ACTIVITY-statement with its references to a PARTICIPANT and a piece of DATA.

TABLE II
SEPL ASSIGNMENT

```
ACTIVITY     a_005
    NAME     incoming-procedure
    DESCRIPTION   tasks that are performed after
                  arrival of reimb'-claim at
                  the GP's local rep'
    PERFORMER p_003  // input-staff
    DATA_USED o_002  // floppy-disk
              o_003  // reimburse'-record
    IMPLEMENTATION MANUAL
    SECURITY_LEVELS
        CONFIDENTIALITY   VERY HIGH
        INTEGRITY         MEDIUM
        AVAILABILITY      LOW
        ACCOUNTABILITY    HIGH
    END_SECURITY_LEVELS
END_ACTIVITY
//..
DATA o_002
    NAME floppy-disk
//..
DATA o_003
    NAME reimburse'-record
//..
PARTICIPANT p_003
    NAME input-staff
//..
```

As certain safeguards only make sense for special kinds of components, type markings will be used to decide whether a safeguard should be implemented for a process component or not; e.g. data kept on storage media can be encrypted whereas data on a piece of paper cannot. Activities can optionally be marked with TRANSFER for data transmission, STORAGE when data is stored, or MANUAL when no computer systems are used. Actors may be assigned the types HUMAN or SYSTEM; artefacts can be marked with the types DATA for anything that is stored within a computer system or TANGIBLE for tangible goods or objects, e.g. a paper document or a floppy disk.

The order of activities is modeled using the TRANSITION statement, an example of which will be given during the sample application of POSeM in table VII (cf. section IV).

C. Step 3: Consistency Analysis

During this step several checks will be carried out to ensure that the output of step 3 is consistent and non-contradictory. After checking that the SEPL specifications are complete and contain security and clearance levels for all process components, the following kinds of checks are carried out:

[3]The DATA construct is used to model all artefacts of the business process in question, this distinguishes it from its WPDL counterpart where it represents variables of a process or a workflow model definition. Even though the construct's name implies a piece of data (the name is a reminiscent of the WPDL construct RELEVANT DATA) a SEPL artefact can also be something tangible, e.g. a printed letter or a piece of storage media.

[4]Unlike WPDL, SEPL not only assigns a performer to a step within the business process, but also the piece (or pieces) of data that are used during this step.

• PARTICIPANT-ACTIVITY-CHECK: Checks whether the person's clearance levels are high enough to carry out a specific activity.
• ACTIVITY-ARTEFACT-CHECK: Checks whether a certain artefact might be handled during a certain activity.
• PARTICIPANT-ARTEFACT-CHECK: Checks whether the person to handle a certain artefact has high enough clearance levels. Applied to the security objective confidentiality this check mirrors tradional access control rights similar to the one defined by [30].
All checks have to be performed on all existing combinations of actors, activities and artefacts of the process.

In case an inconsistency is found, the SEPL model has to be reviewed in order to produce a consistent model; generally this can done be resolved in two ways:
• Reassignment of a security or clearance level of an involved process component.
• Change of the process, e.g. assignment of activity to a different actor with a higher clearance level or splitting one activity into two separate tasks.
If e.g. an actor's clearance levels are increased, more safeguards will have to be implemented for him which would lead to higher costs. If, on the other hand, the activity's or artefact's security levels are lowered it could lead to a violation of the general security requirements as defined in step 1. The assignment of an activity to a different actor might prove difficult due to the actor's workload. The decision on how to cope with the inconsistency must therefore be made by the person responsible for the business process in question.

Further kinds of consistency checks are possible, but not included in this version of POSeM as presented in this article (cf. V-B). Depending on the rules in RB1 a reassignment to resolve one inconsistency may lead to another one.

The final output of this step is a consistent and non-contradictory SEPL description of the business process.

D. Step 4: Derivation of Generic Security Measures

During this step the appropriate security measures are derived from the SEPL description using the POSeM derivation rules using a rule base RB2. Those security measures that are necessary for the defined implementation level of a security objective and fit the type marking are selected from a comprehensive catalogue.

The language to specify derivation rules contains constructs to define the safeguard's name, a unique identifier, a description, the security levels that are implemented by the safeguard, and optionally a list of other safeguards (i.e. their unique identifiers) which are made obsolete by its higher level of implementation. To describe RB2's derivation rules the data format SMDL (**S**ecurity **M**easure **D**escription **L**anguage) has been developed. It allows to specify different security measures together with the security objectives they implement for different process components and component types. An example SMDL specification is shown in table III.

A standard set of derivation rules will be included in a POSeM implementation; this set, however, can be changed, extended and configured according to the user's needs. Based on the british standard BS7799[5] [32], it differentiates the BS7799 controls into safeguards for different implementation levels of security and assigns security levels to them. An example would be the control encryption as defined in section 10.3.2 of BS7799. The different *implementation levels* that were defined for RB2 are: simple encryption, 40 bit symmetric encryption, 56 bit symmetric encryption, and 128 bit symmetric encryption.

A safeguard has to be implemented for an actor (participant), artefact (object), or activity if its value within the derivation rule is lower or equal to the one specified for the component in question. E.g., an actor has been assigned the confidentiality value `MEDIUM`, all safeguards have to be implemented that show the values `MEDIUM` or `LOW` within the actor-confidentiality statement in the derivation rule. Figure 2 illustrates a sample derivation for a human participant ranked with the confidentiality level `MEDIUM`.

TABLE III
SMDL DEFINITION

```
MEASURE    m10.3.2-d  // BS7799 chapter number
                      // implementation level D
    NAME          encryption-128
    DESCRIPTION   128bit symmetric encryption
    CONFIDENTIALITY   ACTOR     VERY HIGH
                      ACTIVITY  VERY HIGH
                      ARTEFACT  VERY HIGH  DATA
    INTEGRITY         ACTOR     VERY HIGH
                      ACTIVITY  VERY HIGH
                      ARTEFACT  VERY HIGH  DATA
    ACCOUNTABILITY    ACTOR     HIGH
                      ACTIVITY  HIGH
                      ARTEFACT  HIGH       DATA
END_MEASURE
```

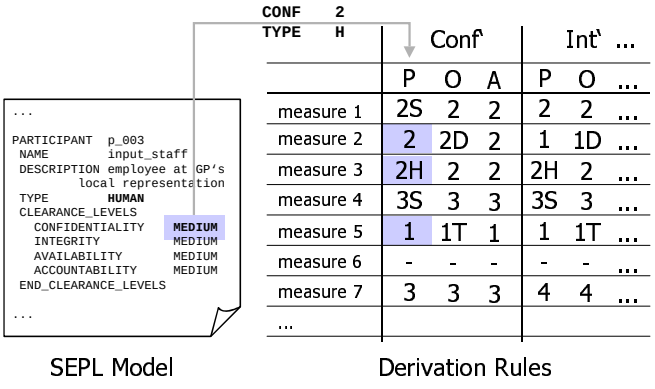

Fig. 2. Sample derivation

[5]Even though BS7799 is generally regarded as a comprehensive reference point for security safeguards other standards with the same goal exist (e.g. [31]) that could also be used as a basis for POSeM's rulebase RB2.

Please note, that all safeguards of RB2 are highly generic, i.e. not specific to certain kinds of computer systems. The result of step 4 are catalogues of safeguards for all process components. If the specified security objectives are to be met, these safeguards have to be implemented.

E. Step 5: Implementation

During the implementation step the generic security measures are mapped to security measures of real systems. To this end existing manuals or security guidelines containing system-specific information can be used, e.g. the Baseline Protection Manual of the GISA[6] [33]. Unlike steps 1 to 4, the tasks during step 5 of POSeM absolutely require a certain familiarity with questions of both IT security and the computer system in question of the user.

If this step is not carried out the results of POSeM, i.e. catalogues of applicable security measures, can still be used when auditing the implementation of IT security for a given business process. The implementation is *not* an integral part of the POSeM method, because POSeM mainly focuses on the analysis of security requirements of a business process.

F. Review

After steps 3, 4, and 5 are completed a review should be carried out in order to analyze whether the security objectives of the process are still in line with those defined for the company. Differences from the initial security objectives might arise if security or clearance levels of participants, artefacts, or actions have been adjusted in order to avoid conflicts during the consistency analysis. It might even be the case that permanent contradictions of aims become obvious.

The review phase after step 3 will also give insight whether the current set-up of the process suits the business's security needs. In some cases it might become obvious that certain parts of the process should be changed — even though it is not the aim of the POSeM method to change the underlying process itself.

Furthermore, after the safeguard catalogues have been generated, i.e. after step 4, the review phase may be used to check whether the current implementation suits the process's security needs as derived by POSeM or if a different but adequate implementation of security is reached.

IV. Example Process

In this chapter an example process will be analyzed using the POSeM method. The process is taken from the field of health care, describing the processing of reimbursement claims of general practitioners (GPs) to their local representation similar to the one customary in Germany.

At the end of each quarter the GP prepares all of his reimbursement claims, sorts them in the appropriate manner, and sends them to his or her local representation. The claims can either be written or printed on special forms or stored on a floppy disk in a defined ASCII-based format [34]. Today, either is sent by regular mail. For means of this article we will only regard the case using floppy disks. At the local representation the data are checked for syntactical correctness and loaded into the local computer system. Before being forwarded the data are checked for plausibility, whether certain rules of the reimbursement system are kept and compiled with other GPs' data into one file per insurance company. Figure 3 gives an overview of the process activities. To illustrate the first four steps of

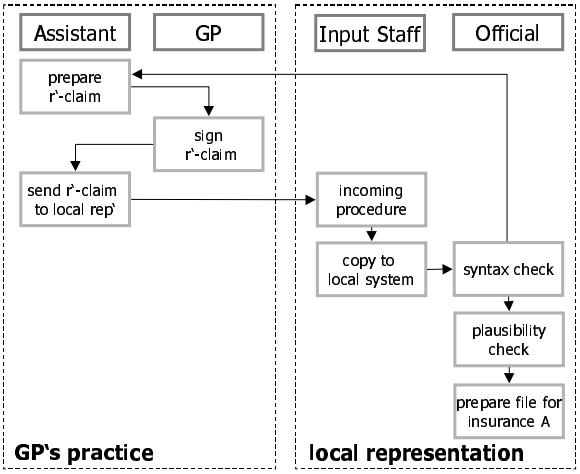

Fig. 3. The reimbursement process

the POSeM method we will examine the actors, artefacts and activities that are concerned when the data on floppy disk first arrive at the GP's local representation.

A. Step 1: General Security Objectives

During step 1 we will analyze in general terms the security objectives and their levels for the given business process. Generally, the following observations can be made.

- **Confidentiality:** In health care many sensitive data are processed, leading to high requirements on the confidentiality of data. Traditionally, the need for confidentiality stems from national data protection legislation and the professional secret of medical staff [14]. Within the reimbursement claims there are diagnoses and medical treatments together with the names and addresses of the GP's patients, i.e. information protected by the professional secret of medical staff and various data protection laws. Therefore the confidentiality is of high importance.

For means of this process we define that any data containing reference to a natural person (i.e. the patient) will be assigned a confidentiality level of `HIGH`. If any match between a person and his or her medical data (e.g. diagnoses) can be made confidentiality will be rated `VERY HIGH`.

- **Integrity:** In health care industry patient data may generally be needed for diagnoses and medication purposes; its integrity is therefore very important.

However, the data processed during our example process are not used for further treatment of the patients but for the reimbursement of the GP. Changes within the data

[6] **G**erman **I**nformation **S**ecurity **A**gency (Bundesamt für die Sicherheit in der Informationstechnik (BSI))

may hurt the plausibility of the GP's claim and therefore have a financial impact for the GP, albeit a small one. The integrity of this kind of data will therefore be rated MEDIUM.

• **Availability:** Generally, in a medical environment the availability of computer systems is of paramount importance. In [35] Anderson cites the case of the collapse of the London Ambulance Service in October and November 1992. Due to the overload and collapse of a new computerized dispatching system, London was left with partial or no ambulance cover for longer periods, which is believed to have led to a loss of about 20 lives.
Nonetheless, the business process in question uses computer systems only for accounting purposes. Short outages of the system could be tolarated and availability is only of minor relevance, i.e. it will stay at LOW to MEDIUM level throughout the process.

• **Accountability:** In health care accountability is needed when is necessary to establish who performed a certain service at a certain time or to prove that a person was allowed to perform a certain service, e.g. to write a prescription. Today, manual signatures of the responsible person ensure this kind of accountability.
In the business process regarded here it must be ensured that the claims are sent in by the GP before a certain deadline and that the data are only controlled by the responsible person. Therefore, accountability is rather important; it will be rated HIGH if a manual signature would be used and otherwise MEDIUM.

B. Step 2: SEPL Model

To create a SEPL model all participants, artefacts, and activities of the process must be regarded. For the subprocess in question only types of persons are involved: An input person (input-staff), who records the incoming date of the floppy disks and copies the data from the floppy disks to the internal computer system, and an official (official) who checks the data for the syntactical correctness and checks the plausibility of the reimbursement claims. Afterwards the data is sorted by special software (localrep-sw) that removes references to the patients, groups it by insurance companies, and prepares files to be send. The clearance levels of these process participants are shown in table IV.

TABLE IV
CLEARANCE LEVELS FOR SELECTED PROCESS PARTICIPANT

	input-staff	official	localrep-sw
Conf'	MEDIUM	VERY HIGH	HIGH
Int'	MEDIUM	MEDIUM	MEDIUM
Av'	LOW	LOW	LOW
Acc'	MEDIUM	HIGH	MEDIUM
mark	HUMAN	HUMAN	SYSTEM

As the input person performs rather clerical tasks his or her security levels are kept low, thus keeping down the cost of information security for this type of employee. Contrarily, the official has a higher responsibility and higher clearance levels.

The following activities can be identified: When the data arrive on floppy disks, their receipt is recorded (incoming-proc') and the files are loaded into a system (copy-to-system). Afterwards the files are automatically checked for syntactical correctness (syntax-check). Having passed that test they are checked for plausibility (plausi'-test). For the activities the security levels are defined as shown in table V:

TABLE V
SECURITY LEVELS FOR SELECTED PROCESS ACTIVITIES

	incoming-proc'	copy-to-system	syntax-check	plausi'-test
Conf'	MEDIUM	MEDIUM	HIGH	HIGH
Int'	MEDIUM	MEDIUM	MEDIUM	MEDIUM
Av'	MEDIUM	MEDIUM	LOW	LOW
Acc'	MEDIUM	MEDIUM	MEDIUM	HIGH
mark	MANUAL	STORAGE	-	-

Since the recording of the incoming data of the GP's claim is important, the availability of incoming-proc' is set to the value MEDIUM.

As to the process artefacts two different kinds can be identified: Artefacts containing data refering to a patient (floppy-disks, and reimburse'-records) and anonymized data (insurance-records) which does not contain demongraphic data of specific patients but still references to the GP who treated the patient. Their security levels are shown in table VI.

TABLE VI
SECURITY LEVELS FOR SELECTED PROCESS ARTEFACT

	floppy-disk	reimburse'-record	insurance-record
Conf'	VERY HIGH	VERY HIGH	HIGH
Int'	MEDIUM	MEDIUM	MEDIUM
Av'	LOW	LOW	LOW
Acc'	HIGH	MEDIUM	HIGH
mark	TANGIBLE	DATA	DATA

Within the process only one loop exists, all other tasks are performed sequentially one after another. The loop occurs just after the syntax-check (activity a_007) is performed and only if a syntax error is found. Then a message to the GP is generated containing the error description and asking the GP for a new floppy-disk with a correct reimbursement file (activity a_007a). The corresponding TRANSITION statement is given in table VII.

C. Step 3: Consistency Analysis

According to the process description, the triplets of actors, activities and artefacts shown in table VIII exist for

TABLE VII
TRANSITION LEADING TO LOOP

```
TRANSITION   t_007
    FROM     a_007 TO a_008
        CONDITION syntax = OK
        FROM a_007 TO a_007a
END_TRANSITION

TRANSITION   t_007a
    DESCRIPTION error message is sent back to
        GP with demand for correct file
    FROM    a_007 TO a_001
END_TRANSITION
```

the given subprocess. Regarding the tables above, the security requirements of the process focus on confidentiality, and the highest variations in requirements can be found for that security objective. Therefore, we will regard their confidentiality levels that are indicated in the row below each triplet:

TABLE VIII
PROCESS "TRIPLETS" AND THEIR CONFIDENTIALITY LEVELS

Actor	Activity	Artefact
input-staff	incoming-proc'	floppy-disk
MEDIUM	MEDIUM	VERY HIGH
input-staff	incoming-proc'	reimburse'-record
MEDIUM	MEDIUM	VERY HIGH
input-staff	copy-to-system	floppy-disk
MEDIUM	MEDIUM	VERY HIGH
official	syntax-check	reimburse'-record
VERY HIGH	HIGH	VERY HIGH
official	plausi'-test	reimburse'-record
VERY HIGH	HIGH	VERY HIGH

Several inconsistencies come up when performing the ACTIVITY-ARTEFACT-CHECK. It shows that all tasks handle artefacts with a higher confidentiality level. Since it would hurt the overall security objectives for artefacts containing patient information to lower the artefacts' confidentiality levels, the activities' confidentiality levels have to be raised accordingly, i.e. raised to VERY HIGH.

Furthermore, the task to load data into the system, i.e. to handle the floppy-disks, is assigned to an input person (input-staff). The PARTICIPANT-ARTEFACT-CHECK reveals a conflict between the confidentiality and accountability levels, because this actor is only allowed to handle medium confidentiality and accountability artefacts whereas the floppy disk was assigned higher security levels.

As a solution one would either reconsider the security level of the artefact or adjust the clearance level of the actor, i.e. assign more responsibility to the input-staff. Adjusting the security objectives of the artefact, i.e. set the confidentiality level of floppy-disk to MEDIUM, would result in a conflict with the overall security objectives and is therefore not acceptable. Another solution would be to assign all tasks where the tasks floppy-disk is handled to the official who handles the data during the next process step. But this would increase the officials' workload substantially and could not be handled by them. Therefore, we decide that the activities in question will not be reassigned, but the input staff's clearance levels will be raised, i.e. the confidentiality level will be set to VERY HIGH and the accountability level will be set to HIGH.

D. Step 4: Derivation of Security Measures

This section will show what kind of security measures have to be implemented for the different process components after the consistency analysis has resulted in a consistent SEPL model. The following paragraphs will explain some example safeguards that should be implemented to secure the given business process. For the derivation of appropriate safeguards the rules defined in table X in the appendix were used. Most safeguards in this list serve the security objective confidentiality, a fact that reflects its importance as analyzed during step 1 of POSeM.

Since the confidentiality levels of the input-staff were raised during the consistency check, user training measures now include both awareness training and training on security requirements and legal responsibilities. Without this raise of confidentiality levels during step 3 only officials would have had the latter training. For all employees confidentiality agreements should be drawn up; security should be included in each employee's job description, i.e. responsibilities for the maintaining security policy as well as for the protection of particular assets.

As to the protection of process's artefacts both floppy-disks and reimburse'-records have to be encrypted using 128bit symmetrical encryption. Furthermore standards and procedures for key management should be applied.

A safeguard that appears in the catalogue for the copy-to-system activity is the scan for computer viruses even if the sender of the files is known. The program used should be updated in regular and short intervals, a policy for file handling should exist and apply to all artefacts, actors and activities of the business process.

The following listing shows all those safeguards that would be selected from table X for a human participant with MEDIUM confidentiality level, such as input-staff before the consistency analysis:

- security should be included into his or her job responsibilities,
- he or she should take part in an awareness training as part of an information security education,
- he or she should be aware of the policy regarding file handling, workplace anti-virus software should be installed and upgraded with each available update, incoming files of any origin (i.e. files obtained from GPs' floppy disks) should be checked for viruses,

• his or her responsibililities when handling input data should be clearly defined,
• he or she should be aware of a policy on the use of cryptographic controls that address general principals, the approach to key management and a description of roles and responsibilities,
• he or she should use at least 40bit encryption when handling data,
• to prove that he or she was the one that handled a piece of data digital signatures should be used, the certificates can be self-signed and generated by public domain software, and
• he or she should know and apply the defined key management procedures.

However, since his or her confidentiality level was raised to `VERY HIGH` moreover the following safeguards were selected from table X.

• the information security education should also include training on security and legal requirements,
• for encryption of data a longer keylength should be applied, i.e. 128bit, and
• for digital signatures certificates should be used that were signed by a trusted third party (TTP).

A complete list of safeguards as derived from a complete rule base RB2 would include measures concerning physical and environmental security, access control and others [32].

E. Review

After the consistency analysis the security and clearance levels of the process components have not been lowered and do therefore not contradict the general security objectives as defined in step 1. However, certain security levels had to be raised in order to achieve consistency, especially confidentiality levels of some process activities as well as confidentiality and accountability levels of `input-staff`, leading to costly safeguards to be implemented. Since the input persons usually perform clerical tasks, it should be analyzed whether the process could be changed in a way that the `input-staff`'s clearance levels reflect the nature of their tasks without producing inconsistencies, e.g. defining different activities or artefacts in a way that only low-level components are to be handled or executed by input persons.

Furthermore, the lists created during step 4 could be used when auditing the current implementation of the business process for appropriate security. Today, when preparing the floppy disk all confidential data of the reimbursement records are encrypted using a symmetric encryption algorithm (IDEA) with a 128bit key, e.g. the GP's own name and address, the patients' names and addresses, the diagnoses [36]. However, the keys used by the GPs are included within the module that is used for encryption, i.e. all GPs in one local area use the same encryption keys; distinctions between keys are made according to the type of reimbursement claim. The encryption program together with its encryption keys is distributed only on a need-to-have basis.

V. Discussion and Further Research

This paper presented a method for the derivation of appropriate safeguards based on business process models.

A. Application and Advantages

POSeM uses a general security policy of an organization to create a consistent security model that is used to derive generic security mechanisms. It assumes a comprehensive view on security, as it takes into account the four security objectives confidentiality, integrity, availability, and accountability. A differentiated view on these security goals is necessary because a security measure that implements a certain security objective does not implement another one[7]. In extreme cases security goals might even contradict each other.

Generally, the POSeM method as presented in this article can be used in two ways:

• to compile safeguard catalogues for an appropriate security standard of a given business process before its actual set-up within an enterprise,
• to provide a checklist when reviewing or auditing the IT security of a process implementation, when both process and security measures are in place and running.

The method may also be used to provide transparency on how the levels of security objectives reflect on necessary safeguards and thus on implementation costs.

POSeM does not attempt to replace current methods of security management. It is rather a set of methods to help analysts to get a comprehensive list of appropriate security measures, also including organizational measures that need to be supported by an established security management framework. The decision which of these measures must be implemented has still to be taken by a human specialist.

Unlike current methods that use risk and threat analyses to define necessary security safeguards, POSeM is based on security objectives that can be defined by the process owner. Current literature shows that approaches based on risk analysis do not meet the requirements on today's computer systems, as they select safeguards primarily based on the requirements from infrastructure. An analysis that is based on *"the 'amount' of confidentiality, integrity and availability"* is favored by Gerber and von Solms [38] and regarded as more suitable for modern computer systems.

Data that exists within an organization (e.g. after an BPR analysis) is (re-)used for a second purpose, i.e. a security model. This means that data may be used again, thus minimizing effort for the security analysis. Especially information on users and their roles and access rights is recorded for both security and process analysis. Moreover, data structures and storage objects of the security analysis are closely related to the artefacts of a process analysis.

[7] A well-known example is cited by Cohen [37]. He considers a system in which access control is implemented using the Bell-LaPadula-Model [30], i.e. where the confidentiality of programs and documents is guaranteed, and shows that a computer virus can spread from programs of a low classification to programs of higher classifications — thereby compromising the system's integrity.

Table IX shows how data used for process modeling overlaps with information collected for modeling or analyzing security.

TABLE IX
PROCESS VS. SECURITY MODELS

Process Models	Security Models
functional perspective	processes, I/O devices
behavioral perspective	–
organisational perspective	users and user roles
informational perspective	data structures and storage objects
–	security attributes
–	non-disclosure levels

Even though it does not aim to be automatable, SEPL represents a complete process modeling language as it contains the four perspectives of a process description (cf. section II-B). SEPL's `ACTIVITY` statement represents the functional perspective. The behavioral perspective is covered by the `TRANSITION` statements that allow for control structures such as loops and conditions. The organisational perspective is represented by the `PERFORMER` and `DATA_USED` keywords within the `ACTIVITY` statement. The informational perspective is decribed by SEPL's `DATA` statements.

B. Next Steps and Open Issues

In this paper the conceptual basis for security requirements analysis using business process models was developed. Further steps will therefore be concerned with the refinement of POSeM and a prototypical implementation that facilitates the automatable tasks.

One of POSeM's main objectives was applicability. Therefore, it was tried to reduce the complexity of the model, especially in the rule bases and derivation step. Since IT security is such a vast and dynamic issue, several research areas remain to be elaborated further, e.g. for the following issues:

- To formulate more detailed consistency requirements, a language will be developed that allows for the specification of sophisticated rules such as separation of duties. Furthermore formal descriptions of both rule bases will be provided.
- In its current implementation POSeM's rule base RB2 does not distinguish between safeguards that are sufficient to reach a defined protection goal and safeguards that only contribute to it. Furthermore, the model does not take into account that the implementation of several safeguards of a lower level may together implement a higher level of security. In a further step weighted sums could be used to provide alternatives on how security could be implemented for a given business process.
- To allow for a more granular selection of safeguards the underlying security model may be extended. Model extensions may include time as an additional dimension for specifying objectives. E.g. an artefact might be highly confidential in the beginning of the process but loosing this requirement as the process continues. At the moment, this can be modeled by defining different artefacts for different stages of the process. The use of time as a dimension might provide a more sophisticated solution. Other model extensions could be type markings that distinguish between more kinds of process components.

APPENDIX

I. DERIVATION RULES

Table X shows an extract of rule base RB2. The safeguards were taken form BS7799 and assigned implementation levels and derivation rules. To improve readability a table was used as form of presentation. The abbreviations in the title line describe the type of process component: P stands for participant or actor, O is short for object or artefact, and A means action or activity. The numbers in the table's body indicate whether a measure contributes to the aspect of the security goal as follows: 1 (`LOW`), 2 (`MEDIUM`), 3 (`HIGH`), 4 (`VERY HIGH`). Note that the safeguards are taken from the BS7799 but were classified according to security objective and process component in order to allow for derivation rules for security measures.

Letters noted behind a number specify that a safeguard only applies to a certain type of component. Actor types are H (human) and S (system). Objects may be either D (data) or T (tangible). For activities the abbreviations are S (storage), T (transmission) and M (manual). If no letter is denoted the measure applies to all types of actors, activities, or artefacts. The following table contains controls from chapters 6 (Personnel Security), 8 (Communications and Operations Management), and 10 (Systems Development and Maintenance) of the BS7799, but lacks the detailed description of safeguards given in the standard.

REFERENCES

[1] Gary Gaskell, "An Analysis of BS7799 and Requirements for E Commerce," in *Proceedings of the NIST/NIAP Symposium on Requirements Engineering for Information Security*, Indianapolis, March 2001.

[2] Paulo Barthelmess, "Security in Workflow Systems," Universtity of Colorado at Boulder, `http://ugrad-www.cs.colorado.edu/~barthelm/security/`, accessed 11/9/2000, 2000.

[3] Wilfried Thoben, "Sicherheit für Workflow-basierte Anwendungen," in *Sicherheit in Informationssystemen SIS' 98*, Kurt Bauknecht, Alfred Büllesbach, Hartmut Pohl, and Stephanie Teufel, Eds., Stuttgart, März 1998, pp. 201–222, vdf Hochschulverlag AG.

[4] Hartmut Jansen, "Integration von Bedrohungs- und Risikoanalyse in ein Vorgehensmodell für Geschäftsprozeßmodellierung und Workflow-Management," M.S. thesis, Fachbereich Informatik der Carl von Ossietzky-Universität Oldenburg, 1998.

[5] Peter Konrad, *Geschäftsprozess-orientierte Simulation der Informationssicherheit: Entwicklung und empirische Evaluierung eines Systems zur Unterstützung des Sicherheitsmanagements*, vol. 20 of *Reihe Wirtschaftsinformatik*, Josef Eul Verlag GmbH, 1998.

[6] Dimitris Karagiannis and Mark Heidenfeld, "Modellierung, Analyse und Evaluation sicherer Geschäftsprozesse: Ein Implementierungsansatz für Security Workflows," in *Sicherheit in Informationssystemen — SIS'98*, Kurt Bauknecht, Alfred Büllesbach, Hartmut Pohl, and Stephanie Teufel, Eds. 1998, pp. 223–246, vdf Hochschulverlag AG an der ETH Zürich.

[7] Alexander W. Röhm, Gaby Herrmann, and Günther Pernul, "A Language for Modelling Secure Business Transactions," in *Proc. 15th Annual Computer Security Applications Conference*, Phoenix, Arizona, December 1999, IEEE Computer Society Press.

TABLE X

EXAMPLE DERIVATION RULES

Measure / Safeguard (with BS7799 chapter number)	Confidentiality			Integrity			Availability			Accountability		
	P	O	A	P	O	A	P	O	A	P	O	A
6.1 security in job definition and resourcing												
• including security in job responsibilities	2H	2	2	3H	3	3	3H	3	3	3H	3	3
• personnel screening and policy	3H	3	3	-	-	-	-	-	-	3H	3	3
• confidentiality agreements	3H	3	3	-	-	-	-	-	-	3	3	3
...												
6.2 user training												
• information security education												
- awareness training	2H	2	2	2H	2	2	2H	2	2	2H	2	2
- on security requirements and legal responsibilities	3H	3	3	3H	3	3	3H	3	3	3H	3	3
...												
8.3 protection against malicious SW												
• policy regarding file handling	1H	1	1	2H	2	2	2H	2	2	-	-	-
• installation, update of AV-SW												
- with each update	2	2	2	2	2	2	2	2	2	2	2	2
- once per month	1	1	1	1	1	1	1	1	1	1	1	1
• check incoming files												
- of unknown origin	1	1D	1S	1	1D	1S	1	1D	1S	1	1D	1S
- any incoming files	2	2D	2S	2	2D	2S	2	2D	2S	2	2D	2S
...												
10.2 security in application systems												
10.2.1 input data validation												
• proc's for responding to validation errors	-	-	-	2	2	2	-	-	-	-	-	-
• proc's for plausibility testing	-	-	-	2	2D	2	-	-	-	-	-	-
• defining responsibilities of "input" staff	2	2	2	2	2	2	2	2	2	-	-	-
...												
10.3 cryptographic controls												
10.3.1 policy on use of cryptographic controls												
• description of general principles	2	2	2	2	2	2	-	-	-	2	2	2
• description of approach to key man'	2	2	2	2	2	2	-	-	-	2	2	2
• description of roles and responsibilities	2H	2	2	2H	2	2	-	-	-	2H	2	2
10.3.2 encryption												
• simple encryption	1	1D	1	-	-	-	-	-	-	-	-	-
• 40 bit symmetric encryption	2	2D	2	2	2D	2	-	-	-	1	1D	1
• 56 bit symmetric encryption	3	3D	3	3	3D	3	-	-	-	2	2D	2
• 128 bit symmetric encryption	4	4D	4	4	4D	4	-	-	-	3	3D	3
10.3.3 digital signatures												
• public domain software (any keylength)	2	2D	2	3	3D	3	-	-	-	3	3D	3
• TTP certified key (hard disk, 2048 bit)	3	3D	3	4	4D	4	-	-	-	4	4D	4
• TTP certified key (smart card, 2048 bit)	4H	-	-	4H	-	-	-	-	-	4H	-	-
...												
10.3.5 key management												
• protection of crypto' keys	2	2	2	3	3	3	-	-	-	2	2	2
• standards, procedures, and methods	2	2	2	3	3	3	-	-	-	2	2	2

[8] Gaby Herrmann, "Security and Integrity Requirements of Business Processes — Analysis and Approach to Support their Realisation," in *Proc. CAiSE*99, 6th Doctoral Consortium on Advanced Information Systems Engineering*, Heidelberg, June 1999, pp. 36–47.

[9] Lawrence Chung, "Dealing with Security Requirements During the Development of Information Systems," in *Advanced Information Systems Engineering, CAiSE*93*, Colette Rolland, François Bodart, and Crorine Cauvet, Eds., Paris, France, June 1993, vol. 685 of *Lecture Notes in Computer Science*, pp. 234–251, Springer.

[10] John McDermott and Chris Fox, "Using Abuse Case Models for Security Requirements Analysis," in *15th Annual Computer Security Applications Conference (ACSAC)*, Phoenix, Arizona, December 1999, `http://www.acsac.org/1999/abstracts/wed-b-1030-john.html`.

[11] Ralph Holbein, *Secure Information Exchange in Organisations — An approach for solving the information misuse problem*, Ph.D. thesis, Universität Zürich, 1996.

[12] Ralph Holbein, Stephanie Teufel, and Kurt Bauknecht, "The Use of Business Process Models for Security Design in Organizations," in *Information System Security — Facing The Information Society of The 21th Century (IFIP/SEC'96)*, S. K. Katsikas and D. Gritzalis, Eds. 1996, Chapman & Hall.

[13] Susanne Röhrig, Franziska Schneider, and Konstantin Knorr, "Sicherer IT-Einsatz im Gesundheitswesen: Abschlussbericht des SNF-Projektes MobiMed (Privacy and Efficiency of Mobile Medical Systems)," Tech. Rep., Universität Zürich, Institut für Informatik, Mai 2000, `http://www.ifi.unizh.ch/ikm/mobimed`.

[14] Susanne Röhrig and Konstantin Knorr, "Towards a Secure Web-Based Health Care Application," in *Proceedings of the 8th European Conference on Information Systems : ECIS 2000 — A Cyberspace Odyssey*, Hans Robert Hansen, Martin Bichler, and Harald Mahrer, Eds., July 2000, vol. 2, pp. 1323–1330.

[15] Konstantin Knorr and Susanne Röhrig, "Security Requirements for E-Commerce Processes," in *Towards the E-Society: E-Commerce, E-Business and E-Government*, Beat Schmid, Katarina Stanoevska-Slabeva, and Volker Tschammer, Eds., Zurich, Switzerland, October 2001, pp. 73–86, Kluwer Academic Publishers.

[16] Susanne Röhrig, Konstantin Knorr, and Hansrudi Noser, "Sicherheit von E-Business-Anwendungen — Struktur und Quantifizierung," *Wirtschaftsinformatik*, vol. 42, no. 6, pp. 499–507, 2000.

[17] Arion Meier and Susanne Röhrig, "Sicherheitsanforderungen für elektronische Verträge: Ein prozessbasierter Ansatz," in *Elek-*

tronische Geschäftsprozesse — Grundlagen, Sicherheitsaspekte, Realisierungen, Anwendungen, Patrick Horster, Ed. September 2001, IT Security & IT Management, pp. 242–253, it Verlag.

[18] Marschall D. Abrams, Sushil Jajodia, and Harold J. Podell, Eds., *Information Security: An Integrated Collection of Essays*. IEEE Computer Society Press, 1995.

[19] R. Shirey, "Internet Security Glossary," Request for Comments 2828, May 2000.

[20] Department of Commerce, National Bureau of Standards, *Guidelines for Security of Computer Application, Federal Information Processing Standards Publication 73*, June 1980.

[21] Gurpreet Dhillon and James Backhouse, "Information System Security Management in the New Millennium," *Communications of the ACM*, vol. 43, no. 7, pp. 125–128, July 2000.

[22] Ross J. Anderson, *Security Engineering — A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, 2001.

[23] National Computer Security Center, *NCSC-TG-004: Glossary of Computer Security Terms (Teal Green Book)*, October 1988, `http://www.fas.org/irp/nsa/rainbow/tg004.htm`.

[24] National Computer Security Center, *NCSC-TG-010: A Guide to Understanding Modeling in Trusted Systems (Acqua Book)*, October 1992.

[25] T.H. Davenport, *Process Innovation — Reengineering Work through Information Technology*, Harvard Business School Press, Boston, 1993.

[26] Michael Hammer and James Champy, *Reengineering the Coroation — a Manifest for Business Revolution*, Nicholas Brealey, London, 1994.

[27] Reidar Conradi, Christer Fernström, and Alfonso Fuggetta, "Concepts for Evolving Software Processes," in *Software Process Modelling and Technology*, Anthony Finkelstein, Jeff Kramer, and Bashar Nuseibeh, Eds., pp. 9–31. Research Studies Press Ltd., 1994.

[28] Bill Curtis, Marc I. Kellner, and Jim Over, "Process Modeling," *Communications of the ACM*, vol. 35, no. 9, pp. 75–90, 1992.

[29] Workflow Management Coalition, *Interface 1: Process Definition Definition Interchange — Process Model*, 1998, Document Number TC-1016-P.

[30] David E. Bell and Leonard J. LaPadula, "Secure computer systems: Mathematical foundations and model," Tech. Rep., The Mitre Corporation, 1974.

[31] "The Forum's Standard of Good Practice: The Standard for Information Security," `http://www.securityforum.org`, November 2000.

[32] BSI: British Standards Institute, *Information Security Management — Part 1: Code of practice for information security management*, 1999.

[33] Bundesamt für die Sicherheit in der Informationstechnik (BSI), Bonn, *IT-Grundschutzhandbuch: Maßnahmenempfehlungen für den mittleren Schutzbedarf*, Januar 2000.

[34] "KVDT Datensatzbeschreibungen: Einheitlicher Datenaustausch zwischen Arztpraxis und Kassenärztlicher Vereinigung," `http://www.kbv-it.de`, accessed 18/11/2001, November 2001.

[35] Ross J. Anderson, "Information technology in medical practice: safety and privacy lessons from the United Kingdom," *Australian Medical Journal*, 2000, `http://www.cl.cam.ac.uk/users/rja14/`.

[36] "KBV-Kryptomodul: Handbuch für die Version 2.14," `http://www.kbv-it.de`, accessed 18/11/2001, November 2001.

[37] Frederic B. Cohen, *A Short Course on Computer Viruses*, Wiley Professional Computing. John Wiley & Sons, second edition, 1994.

[38] Mariana Gerber and Rossouw von Solms, "From Risk Analysis to Security Requirements," *Computers & Security*, vol. 20, pp. 577–584, 2001.